GUIDE PRATIQUE RGPD

SÉCURITÉ DES DONNÉES PERSONNELLES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

TABLE DES MATIÈRES

AVANT-PROPOS

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 121 de la loi Informatique et Libertés[1]). Le règlement général sur la protection des données[2] (RGPD) précise que la protection des données personnelles nécessite de prendre les « *mesures techniques et organisationnelles appropriées afin de garantir un* ***niveau de sécurité adapté au risque*** ». Cette exigence s'impose aussi bien au responsable du traitement de données personnelles qu'aux sous-traitants impliqués (article 32 du RGPD).

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 n'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 œuvre.

Pour vous aider dans votre mise en conformité, **ce guide rappelle les précautions élémentaires qui devraient être mises en œuvre de façon systématique.** Ce guide est notamment destiné aux DPO (délégués à la protection des données), RSSI (responsables de la sécurité des systèmes d'information) et informaticiens. Les juristes et les utilisateurs pourront également y trouver des éléments utiles.

Dans l'idéal, ce guide sera utilisé dans le cadre d'une gestion des risques, même minimale, constituée des trois actions suivantes.

1. Recenser les traitements de données personnelles, automatisés ou non, les données traitées (ex. : fichiers clients, contrats) et les supports sur lesquels ces traitements reposent :

- les matériels (ex. : serveurs, ordinateurs portables, disques durs) ;
- les logiciels (ex. : systèmes d'exploitation, logiciels métier) ;
- les canaux de communication logiques ou physiques (ex. : fibre optique, Wi-Fi, Internet, échanges verbaux, coursiers) ;
- les supports papier (ex. : documents imprimés, photocopies) ;
- les locaux et installations physiques où se situent les éléments précédemment cités (ex. : locaux informatiques, bureaux).

2. Apprécier les risques engendrés par chaque traitement :

a. Identifier les impacts potentiels sur les droits et libertés des personnes concernées, pour les trois évènements redoutés suivants :

- **accès illégitime à des données** (ex. : usurpation d'identité consécutive 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).

1 « La loi Informatique et Libertés », cnil.fr

2 « Le règlement général sur la protection des données - RGPD », cnil.fr

b. **Identifier les sources de risques** (qui ou qu'est-ce qui 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) ainsi que des sources non humaines internes et externes (ex. : eau, épidémie, matériaux dangereux, virus informatique non ciblé).

c. **Identifier les menaces réalisables** (qu'est-ce qui pourrait permettre que chaque évènement redouté survienne ?). Ces menaces surviennent sur les supports identifiés précédemment (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 déni de service).

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

e. **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 pour les personnes	Vraisem-blance
Accès illégitime à des données						
Modification non désirée de données						
Disparition de données						

3. **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. Sinon, des mesures supplémentaires doivent être décidées et mises en place pour abaisser la gravité et/ou la vraisemblance des risques associés.

POUR ALLER PLUS LOIN

- Le RGPD introduit les **analyses d'impact relatives à la protection des données** (AIPD) et précise que celles-ci doivent au moins contenir *« une description [...] des opérations [...] et des finalités du traitement [...], une évaluation de la nécessité et de la proportionnalité [...], une évaluation des risques [...] et les mesures envisagées pour faire face aux risques [...] et visant à apporter la preuve du respect du règlement »* (voir article 35.7). **La réflexion sur les risques dont il est question dans cette fiche permet d'alimenter le volet sur l'appréciation des risques de l'analyse d'impact.**
- Les guides AIPD de la CNIL[3] permettent de mener une analyse d'impact relative à la protection des données. La CNIL a également publié un logiciel pour faciliter la conduite et la formalisation d'AIPD[4].
- **Les audits de sécurité sont un moyen essentiel pour évaluer le niveau de sécurité d'un traitement de données personnelles.** Réalisés de façon périodique, ils permettent de prendre en compte les évolutions du traitement et des menaces. Chaque audit doit donner lieu à un plan d'action dont la mise en œuvre devrait être suivie au plus haut niveau de l'organisme.
- **L'étude des risques sur la sécurité de l'information[5] 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.

3 « Les guides AIPD (analyse d'impact relative à la protection des données) », cnil.fr

4 « Outil PIA : téléchargez et installez le logiciel de la CNIL », cnil.fr

5 Par exemple à l'aide de la méthode EBIOS RM (voir : « La méthode EBIOS Risk Manager », ssi.gouv.fr), la 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.

FICHE 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 (aussi bien internes qu'externes à l'organisme) travaillant avec des données personnelles aux risques liés aux libertés et à la vie privée des personnes,** les informer des mesures prises pour traiter ces risques et des conséquences potentielles en cas de manquement. Concrètement, il peut s'agir d'organiser une séance de sensibilisation, d'envoyer régulièrement les mises à jour des procédures pertinentes pour les personnes selon leurs fonctions, de 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 personnelles, qu'il s'agisse d'une opération 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 et la politique de mots de passe que l'utilisateur doit respecter ;
   - 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, toute perte ou vol de matériel 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 et leur paramétrage 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 télécommunication 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'accès à Internet ;
   - la messagerie électronique ;
   - la téléphonie.

4. Les conditions d'administration du système d'information, et l'existence, le cas échéant, de :
   - systèmes automatiques de filtrage ;
   - systèmes automatiques dédiés à la traçabilité des actions ;
   - systèmes de 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 (ex. : public, interne, confidentiel) et imposant un marquage des documents, des supports et des e-mails contenant des données confidentielles.
- Ajouter une mention visible et explicite sur chaque page des documents papier ou électroniques qui contiennent des données sensibles[6].
- 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. Les campagnes de sensibilisation peuvent également prendre la forme de simulations d'attaque (ex. : campagnes d'hameçonnage ou « *phishing* »).
- Prévoir la signature d'un **engagement de confidentialité** (voir modèle de clause ci-contre), ou prévoir dans les contrats de travail une **clause de confidentialité spécifique** concernant les données personnelles.

6 Les données sensibles sont décrites à l'article 6 de la loi Informatique et Libertés et à l'article 9 du RGPD.

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

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 à l'article 32 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes à l'état de l'art et aux règles internes 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 à l'état de l'art et aux règles internes dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes à l'état de l'art et aux règles internes 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 règlementation en vigueur, notamment au regard des articles 226-13 et 226-16 à 226-24 du code pénal.

Fait à xxx, le xxx, en xxx exemplaires

Nom :
Signature :

FICHE 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 :

- **un facteur de connaissance** (ce que l'on sait), par exemple un mot de passe ;
- **un facteur de possession** (ce que l'on a), par exemple une carte à puce ;
- **un facteur inhérent** (ce que l'on est) qui peut être biométrique, par exemple une empreinte digitale, ou comportementale[7], par exemple la frappe au clavier. Pour rappel, le traitement de données biométriques visant à identifier un individu automatiquement et de manière unique à partir de ses caractéristiques physiques, physiologiques ou comportementales est un traitement de données sensibles donnant lieu à l'application de l'article 9 du RGPD[8].

L'authentification d'un utilisateur est qualifiée de multifacteur lorsqu'elle a recours à une combinaison d'au moins deux de ces catégories et est dite forte si un facteur au moins repose sur un mécanisme cryptographique robuste (ex. : clé cryptographique).

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, mettre en œuvre des moyens pour tracer les actions associées à ces identifiants et renouveler le mot de passe dès qu'une personne n'a plus besoin d'accéder au compte.
- **Respecter la recommandation de la CNIL[9] dans le cas d'une authentification des utilisateurs basée sur des mots de passe,** notamment en appliquant les règles suivantes :
  - **conserver de façon sécurisée les mots de passe** ;
  - ne pas demander le renouvellement périodique des mots de passe pour les simples utilisateurs (au contraire des administrateurs) ;
  - obliger l'utilisateur à **changer**, dès sa première connexion, **tout mot de passe attribué automatiquement ou par un administrateur** lors de la création du compte ou d'un renouvellement du mot de passe ;
  - imposer une complexité en fonction des cas d'usage :
    - **par défaut, entropie** (imprédictibilité théorique) **minimale de 80 bits** (ce qui correspond par exemple à 12 caractères minimum comportant des majuscules, des minuscules, des chiffres et des caractères spéciaux ou bien 14 caractères minimum comportant des majuscules, des minuscules et des chiffres, sans caractère spécial obligatoire) ;

7 L'authentification comportementale est une technologie moins mature que la biométrie par exemple.

8 En matière d'authentification sur le lieu de travail, cela se traduit par l'obligation, pour tout responsable de traitement souhaitant mettre en œuvre un tel traitement, de se conformer aux dispositions du règlement type relatif à l'accès par authentification biométrique sur les lieux de travail (voir : « Le contrôle d'accès biométrique sur les lieux de travail », cnil.fr).

9 « Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité », cnil.fr

- entropie de 50 bits dans le cas où des mesures complémentaires sont en place (restriction de l'accès au compte telle qu'une temporisation de l'accès après plusieurs échecs, la mise en place de « Captcha » ou le blocage du compte après 10 échecs) ;
- entropie de 13 bits dans le cas d'un matériel détenu par l'utilisateur (ex. : carte SIM, dispositif contenant un certificat) avec blocage au bout de 3 échecs.

Vérifier la robustesse de sa politique de mots de passe.
La CNIL met à disposition sur son site web un outil[10] pour calculer la complexité des mots de passe demandés aux utilisateurs, selon chaque cas d'usage (mot de passe seul, avec restriction d'accès ou avec un matériel détenu par la personne).

Afin de créer des mots de passe complexes, il est possible de s'appuyer sur l'un des deux moyens suivants :

- **Les moyens mnémotechniques,** par exemple en :
  - ne conservant que les premières lettres des mots d'une phrase créée pour l'occasion ;
  - mettant une majuscule si le mot est un nom (ex. : Chef) ;
  - gardant des signes typographiques et de ponctuation (ex. : ') ;
  - exprimant les nombres à l'aide des chiffres de 0 à 9 (ex. : Un → 1) ;
  - utilisant des abréviations phonétiques (ex. : acheté → ht).

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

- **Les gestionnaires de mots de passe**[11], qui :
  - permettent d'enregistrer de façon sécurisée autant de mots de passe que nécessaire tout en n'exigeant la mémorisation que d'un seul mot de passe maître ;
  - proposent de générer des mots de passe aléatoires et, pour certains d'entre eux, d'avoir une estimation de leur entropie ;
  - peuvent remplir automatiquement les champs d'authentification.

Ce qu'il ne faut pas faire

- Communiquer un mot de passe personnel à une autre personne.
- Stocker des mots de passe dans un fichier en clair, sur un papier ou dans un lieu facilement accessible par d'autres personnes.
- Enregistrer les mots de passe dans un navigateur sans mot de passe maître.
- Utiliser des mots de passe ayant un lien avec soi (ex. : nom, date de naissance).
- 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.
- Utiliser une fonction cryptographique conçue en interne qui est, par conséquent, non reconnue ou éprouvée.
- Utiliser une fonction cryptographique obsolète, telle que MD5 ou SHA-1, pour stocker des mots de passe.

10 « Vérifier sa politique de mots de passe », cnil.fr

11 « 5 arguments pour adopter le gestionnaire de mots de passe », cnil.fr

POUR ALLER PLUS LOIN

- **Privilégier l'authentification multifacteur** lorsque cela est possible.
- **Limiter le nombre de tentatives d'accès** aux comptes utilisateur sur les postes de travail et bloquer temporairement le compte lorsque sa limite est atteinte.
- **Imposer un renouvellement du mot de passe** selon une périodicité pertinente et raisonnable pour les administrateurs (uniquement).
- Mettre en œuvre des moyens techniques pour **faire respecter les règles relatives à l'authentification** (ex. : blocage du compte en cas de non-renouvellement du mot de passe d'un administrateur).
- Éviter, si possible, que les identifiants (ou « *logins* ») des utilisateurs et ceux des administrateurs soient ceux des comptes définis par défaut par les éditeurs de logiciels et désactiver les comptes par défaut.
- **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[12] (voir fiche n°17 : Chiffrer, hacher ou signer). Une clé ne doit pas être stockée dans la même base de données que les empreintes générées.
- L'ANSSI a publié avec la collaboration de la CNIL[13] des recommandations relatives à l'authentification multifacteur et aux mots de passe. Se référer également aux guides[14] publiés par l'ANSSI pour aider les développeurs et administrateurs dans leurs choix d'algorithmes cryptographiques, de dimensionnement et d'implémentation.
- Pour les autorités administratives, les annexes du référentiel général de sécurité (RGS)[15] s'appliquent, notamment les annexes B1 et B2 concernant respectivement les mécanismes cryptographiques et la gestion des clés utilisées.

12 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).

13 « Recommandations relatives à l'authentification multifacteur et aux mots de passe », ssi.gouv.fr

14 « Mécanismes cryptographiques », ssi.gouv.fr

15 « Liste des documents constitutifs du RGS v.2.0 », ssi.gouv.fr

FICHE 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.
- **Faire valider toute demande d'habilitation** par un responsable (ex. : supérieur hiérarchique, chef de projet).
- **Supprimer les permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou à une ressource informatique** (ex. : changement de mission ou de poste)**, ainsi qu'à la fin de leur contrat.**
- **Réaliser une revue régulière, a minima 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 à des données personnelles ;
  - les conséquences prévues pour les personnes ayant un accès légitime aux données en cas de non-respect des mesures de sécurité ;
  - les mesures prévues permettant de restreindre et de contrôler l'attribution et l'utilisation des accès au traitement (voir la fiche n°4 : Tracer les opérations et gérer les incidents).

FICHE 4 - TRACER LES OPÉRATIONS ET GÉRER LES INCIDENTS

Tracer les opérations et prévoir les 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

- **S'agissant du suivi des opérations :**
  - **prévoir un système de journalisation** (c'est-à-dire un enregistrement dans des « fichiers journaux » ou « *logs* ») des activités métier des utilisateurs, des interventions techniques (y compris par les administrateurs), des anomalies et des événements liés à la sécurité :
  - **conserver ces évènements sur une période glissante comprise entre six mois et un an** (sauf, par exemple, en cas d'obligation légale, de besoin de gestion des contentieux, de contrôle interne ou encore d'un besoin d'analyse post-incident) ;
  - **effectuer un enregistrement des opérations de création, consultation, modification et suppression** des données en conservant l'identifiant de l'auteur, la date, l'heure et la nature de l'opération ainsi que la référence des données concernées (pour en éviter la duplication) ;
  - **informer les utilisateurs**, par exemple lors de l'authentification ou de l'accès au système, de la mise en place du dispositif de journalisation, après information et consultation des instances représentatives du personnel ;
  - **protéger les équipements de journalisation et les informations journalisées** contre les opérations non autorisées (ex. : en les rendant inaccessibles aux personnes dont l'activité est journalisée), contre les mésusages par des comptes habilités (ex. : en mettant en place une charte d'utilisation ou des alertes spécifiques) et contre l'écrasement des données écrites par les applicatifs concernés ;
  - **s'assurer que les sous-traitants soient contractuellement tenus** de mettre en œuvre la journalisation conformément aux présentes recommandations.
- **S'agissant de la gestion des incidents :**
  - établir des procédures concernant l'analyse des données collectées ainsi que **la génération des alertes et leur traitement en cas de suspicion de comportement anormal** ;
  - s'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** ;
  - prévoir un dispositif de remontée des incidents par les utilisateurs et sensibiliser ces derniers à l'importance de **signaler tout événement suspect** ;

- 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 ;
- **tenir un registre interne de toutes les violations de données personnelles** ;
- **notifier**[16] **à la CNIL, dans les 72 heures, les violations présentant un risque pour les droits et libertés des personnes et,** en cas de de risque élevé et sauf exception prévue par le RGPD[17], **informer les personnes concernées** pour qu'elles puissent en limiter les conséquences[18].

Ce qu'il ne faut pas faire

- Dupliquer et conserver de manière excessive les données personnelles concernées par le traitement au sein des journaux (ex. : y enregistrer les mots de passe ou leur condensat (ou « *hash* ») lors de l'authentification des utilisateurs).
- Utiliser les informations issues des dispositifs de journalisation à d'autres fins que celles de garantir le bon usage du système informatique (ex. : utiliser les traces pour compter les heures travaillées est un détournement de finalité, puni par la Loi).

POUR ALLER PLUS LOIN

- Voir la recommandation de la CNIL relative à la journalisation[19].
- Voir les recommandations de sécurité de l'ANSSI sur le sujet[20].
- Faire participer l'utilisateur à la surveillance des opérations faites sur son compte et ses données (ex. : un récapitulatif des trois dernières connexions).
- Privilégier une surveillance automatique des journaux, couplée à une configuration adaptée des alertes.
- En cas d'incident ou pour s'y préparer, consulter le site d'assistance et prévention en sécurité numérique[21].

16 La procédure de notification est détaillée sur le site de la CNIL (voir : « Notifier une violation de données personnelles », cnil.fr).

17 Articles 33 et 34 du RGPD.

18 L'obligation de notification de violation de données personnelles ne dédouane pas le responsable de ses potentielles autres obligations de remontée d'incident (voir : « Notifications d'incidents de sécurité aux autorités de régulation : comment s'organiser et à qui s'adresser ? », cnil.fr).

19 « La CNIL publie une recommandation relative aux mesures de journalisation », cnil.fr

20 « Recommandations de sécurité pour l'architecture d'un système de journalisation », ssi.gouv.fr

21 « Assistance aux victimes de cybermalveillance », cybermalveillance.gouv.fr

FICHE 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 sur le poste 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.
- Limiter les droits des utilisateurs au strict minimum en fonction de leurs besoins sur les postes de travail.
- **Favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau interne 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.
- **Effacer de façon sécurisée les données présentes sur un poste préalablement à sa réaffectation** à une autre personne.
- Pour les **supports amovibles** (ex. : clés USB, disques durs externes) :
  - sensibiliser les utilisateurs aux risques liés à l'utilisation de support amovibles, en particulier s'ils proviennent de l'extérieur ;
  - **limiter la connexion de supports amovibles** à l'indispensable ;
  - désactiver l'exécution automatique (« *autorun* ») depuis les 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 (ex. : 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 (ex. : affichage d'un message à l'écran).

Ce qu'il ne faut pas faire

- Utiliser des systèmes d'exploitation dont le support n'est plus assuré par l'éditeur.
- Donner des droits à privilèges, en local comme en réseau, aux utilisateurs n'ayant pas de compétence 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.
- Mettre en place une solution d'analyse et de **décontamination des supports amovibles** avant chaque utilisation.
- **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 français de veille, d'alerte et de réponse aux attaques informatiques, publie sur son site web[22] 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.
- Fixer les postes de travail à du mobilier spécifique ou difficilement déplaçable (ex. : utilisation de câbles antivol).
- 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 page[23] du CERT-FR sur les bons réflexes en cas d'intrusion sur un système d'information.

22 « CERT-FR – Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques », cert.ssi.gouv.fr

23 « Les bons réflexes en cas d'intrusion sur un système d'information », cert.ssi.gouv.fr

FICHE 6 - SÉCURISER L'INFORMATIQUE MOBILE

Anticiper l'atteinte à la sécurité des données à l'extérieur des locaux, dont le vol ou la perte d'un équipement mobile.

La multiplication des pratiques de travail hors des locaux de l'organisme (ex. : déplacements, télétravail) comporte des risques spécifiques liés à l'usage d'ordinateurs portables, de clés USB ou encore de smartphones : il est indispensable de les encadrer.

Les précautions élémentaires

- **Sensibiliser les utilisateurs aux risques spécifiques liés à l'utilisation d'outils informatiques mobiles** (ex. : vol de matériel, risques liés à la connexion aux réseaux et équipements non maîtrisés, notamment publics) et aux procédures prévues pour les limiter.
- **Mettre en œuvre des mécanismes maîtrisés de sauvegarde 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 amovibles** (ex. : ordinateur portable, clé USB, disque dur externe, CD-R, DVD-RW) tels que :
  - le chiffrement du disque dur (de nombreux systèmes d'exploitation intègrent une telle fonctionnalité) ;
  - le chiffrement fichier par fichier ;
  - la création de conteneurs (fichier susceptible de contenir plusieurs fichiers) chiffrés.
- **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** (ex. : mot de passe, schéma).
- **Informer les utilisateurs** de la personne à contacter en cas de perte ou de vol de leur matériel.

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.
- **Ne pas laisser d'équipements ou de documents sans surveillance** dans les lieux publics.
- Ne pas discuter (ex. : conversation en groupe ou au téléphone) d'informations sensibles dans les lieux publics.
- **Limiter le stockage des données** sur les postes nomades au strict nécessaire et éventuellement l'interdire lors de déplacement à l'étranger[24].
- **Prévoir des mécanismes de protection contre le vol** (ex. : câble de sécurité, marquage visible du matériel) **et de limitation de ses impacts** (ex. : verrouillage automatique, chiffrement).
- Lorsque des appareils mobiles servent à la collecte de données en itinérance (ex. : assistants personnels, *smartphones*, ordinateurs portables), 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 aussitôt qu'elles ont été transférées au système d'information de l'organisme.

24 « Bonnes pratiques à l'usage des professionnels en déplacement », ssi.gouv.fr

FICHE 7 - PROTÉGER LE RÉSEAU INFORMATIQUE INTERNE

Autoriser uniquement les fonctions réseau nécessaires aux traitements mis en œuvre.

Les précautions élémentaires

- **Limiter les accès Internet** en bloquant les services non nécessaires (ex. : VoIP, pair à pair).
- **Gérer les réseaux Wi-Fi.** Ils doivent utiliser un chiffrement à l'état de l'art (WPA3 ou WPA2 en respectant les recommandations de l'ANSSI sur la configuration de ce dernier[25]) et les réseaux ouverts aux invités doivent être séparés du réseau interne.
- **Imposer un VPN pour l'accès à distance** avec, si possible, une authentification forte de l'utilisateur (ex. : carte à puce, mot de passe à usage unique basé sur le temps (TOTP)).
- **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 (ex. : pare-feux, serveurs proxy et autres). 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

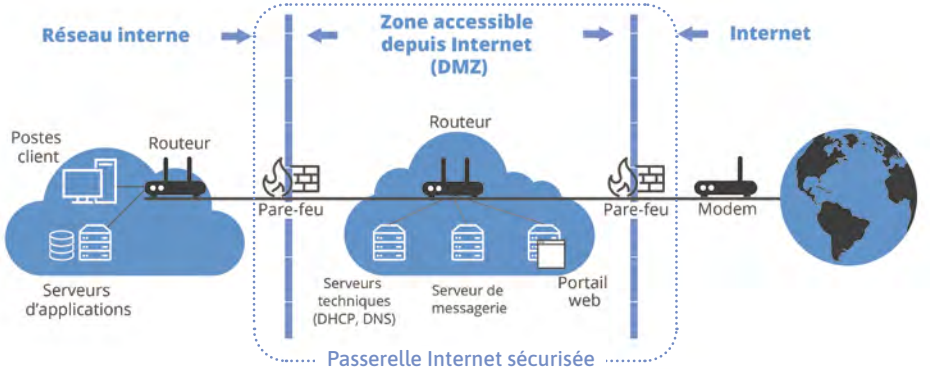
- Utiliser le protocole Telnet pour la connexion aux équipements actifs du réseau (ex. : pare-feux, routeurs, passerelles). Il convient d'utiliser plutôt SSH ou un accès physique direct à l'équipement.
- Mettre à disposition des utilisateurs un accès Internet non filtré.
- Mettre en place un réseau Wi-Fi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

25 « Sécuriser les accès Wi-Fi », ssi.gouv.fr

POUR ALLER PLUS LOIN

- **L'ANSSI a publié des bonnes pratiques**[26], par exemple pour la sécurisation des sites web[27] et la configuration de TLS[28].
- **On peut mettre en place l'identification automatique de matériel** en mettant en place une authentification des matériels (protocole 802.1X) ou, a minima, 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) **et de prévention d'intrusion** (IPS) peuvent analyser le trafic réseau pour détecter des attaques, voire y répondre. **Informer les utilisateurs** de la mise en place de tels systèmes, après information et consultation des instances représentatives du personnel.
- **Le cloisonnement réseau** réduit l'impact 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 (« *gateway* »). À ce sujet, l'ANSSI a publié des recommandations relatives à l'interconnexion d'un système d'information à Internet[29] (desquelles sont inspirées le schéma ci-dessous).

Exemple de mise en œuvre d'une DMZ



26 « Bonnes pratiques », ssi.gouv.fr
27 « Sécuriser un site web », ssi.gouv.fr
28 « Recommandations de sécurité relatives à TLS », ssi.gouv.fr
29 « Recommandations relatives à l'interconnexion d'un système d'information à Internet », ssi.gouv.fr

FICHE 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

- **Désinstaller ou désactiver les services et interfaces inutiles.**
- **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 minimum, lors de chaque départ d'un administrateur et en cas de suspicion de compromission.
- **Installer les mises à jour critiques** sans délai, en particulier les correctifs de sécurité, que ce soit pour les systèmes d'exploitation ou pour les applications, en programmant une vérification automatique hebdomadaire.
- **Utiliser des logiciels de détection et de suppression de programmes malveillants** (ex. : antivirus) régulièrement mis à jour.
- En matière d'administration de base 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 (ex. : attaque par injection de code SQL, scripts).
- **Effectuer des sauvegardes et les vérifier régulièrement** (voir la fiche n°10 : Sauvegarder et prévoir la continuité d'activité).
- **Mettre en œuvre le protocole TLS** (en remplacement de SSL[30]), 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[31].
- **Mettre en place un système de journalisation des événements** sur le serveur (voir la fiche n°4 : Tracer les opérations et gérer les incidents).

Ce qu'il ne faut pas faire

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

30 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.

31 Pour TLS, il existe plusieurs outils à cette fin (ex. : « SSL Server Test », ssllabs.com, « SSL-Tools », ssl-tools.net).

POUR ALLER PLUS LOIN

- Tout système traitant des données sensibles[32] 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 (voir la fiche n°2 : Authentifier les utilisateurs) permettant une traçabilité renforcée (voir la fiche n°4 : Tracer les opérations et gérer les incidents).
- S'agissant des logiciels s'exécutant sur des serveurs, il est conseillé d'utiliser des **outils de détection des vulnérabilités** (logiciels de scans de vulnérabilités tels que nmap[33], nessus[34] ou nikto[35]) 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.
- La version 1.3 de TLS est à privilégier ou, à défaut, la version 1.2 en respectant les recommandations publiées par l'ANSSI sur le sujet[36].
- **L'ANSSI a publié sur son site[37] diverses recommandations** parmi lesquelles la sécurisation de l'administration des systèmes d'information[38] et la mise en place de cloisonnement système[39].

32 Les données sensibles sont décrites à l'article 6 de la loi Informatique et Libertés et à l'article 9 du RGPD.

33 « Nmap », nmap.org

34 « Nessus », tenable.com

35 « Nikto2 », cirt.net

36 « Recommandations de sécurité relatives à TLS », ssi.gouv.fr

37 « Bonnes pratiques », ssi.gouv.fr

38 « Recommandations relatives à l'administration sécurisée des systèmes d'information », ssi.gouv.fr

39 « Recommandations pour la mise en place de cloisonnement système », ssi.gouv.fr

FICHE 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[40]) 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 personnelles.
- **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 administrateur aux équipes en charge de l'informatique interne 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 régulière et les mettre à jour.
- **Limiter les informations renvoyées lors de la création d'un compte utilisateur ou lors de la réinitialisation d'un mot de passe**, afin de ne pas renseigner un attaquant sur l'existence – ou non – d'un compte associé à un identifiant (ex. : adresse de messagerie électronique).

Ce qu'il ne faut pas faire

- Faire transiter des données personnelles dans une URL (ex. : identifiants, mots de passe).
- Utiliser des services non sécurisés (ex. : authentification en clair, flux en clair).
- Utiliser les serveurs comme des postes de travail (ex. : navigation sur des sites web, accès à une messagerie électronique).
- 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).

40 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.

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[41].
- S'agissant des logiciels s'exécutant sur des serveurs, il est conseillé d'utiliser des **outils de détection des vulnérabilités** (logiciels de scans de vulnérabilité tels que nmap, nessus ou nikto) pour les traitements les plus critiques afin de détecter d'éventuelles failles de sécurité. Des systèmes de détection et de 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[42] des recommandations spécifiques** pour mettre en œuvre TLS[43] ou pour sécuriser un site web[44].

41 « Site web, cookies et autres traceurs », cnil.fr

42 « Bonnes pratiques », ssi.gouv.fr

43 « Recommandations de sécurité relatives à TLS », ssi.gouv.fr

44 « Sécuriser un site web », ssi.gouv.fr

FICHE 10 - SAUVEGARDER ET PRÉVOIR LA CONTINUITÉ D'ACTIVITÉ

Effectuer des sauvegardes régulières pour limiter l'impact d'une disparition ou d'une altération 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[45] quotidiennes et des sauvegardes complètes à intervalles réguliers ;
  - **stocker au moins une sauvegarde sur un site extérieur,** si possible dans des coffres ignifugés et étanches ;
  - **isoler au moins une sauvegarde hors ligne**, déconnectée du réseau de l'entreprise ;
  - **protéger les données sauvegardées au même niveau de sécurité que celles stockées sur les serveurs d'exploitation** (ex. : en chiffrant les sauvegardes, en prévoyant un stockage dans un lieu sécurisé, 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 équipements de stockage, par exemple au moyen d'une technologie RAID[46].

45 Une sauvegarde incrémentale consiste à n'enregistrer que les modifications faites par rapport à une précédente sauvegarde.

46 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 consécutive à la panne d'un des supports.

Ce qu'il ne faut pas faire

- Conserver les sauvegardes sur les mêmes systèmes que les données sauvegardées sans les isoler. Une menace informatique (ex. : rançongiciel) pourrait alors s'attaquer aussi bien aux données qu'à leurs sauvegardes.
- 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

- Le Secrétariat général de la défense et de la sécurité nationale (SGDSN) a publié un guide[47] concernant l'établissement d'un plan de continuité d'activité ou de reprise d'activité.
- 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.

47 *Guide pour réaliser un plan de continuité d'activité* (PDF, 1,1 Mo), economie.gouv.fr

FICHE 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 de manière appropriée au regard des risques présentés par l'archivage des données, de la nature des données à protéger et des impacts pour les personnes concernées en cas de violation.

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** puisque l'utilisation d'une archive ne doit intervenir que de manière ponctuelle et exceptionnelle.
- S'agissant de la destruction des archives, **choisir un mode opératoire garantissant que l'intégralité de l'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 ou 5 ans.
- 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 spécialement chargé d'y accéder.

POUR ALLER PLUS LOIN

- La CNIL a publié une recommandation[48] 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 ces problématiques d'archivage sont disponibles sur le site des Archives de France (voir notamment l'article sur la pérennisation de l'information numérique[49]).
- En partenariat avec le Service interministériel des archives de France (SIAF), la CNIL a publié un guide pratique sur les durées de conservation[50].
- 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[51], dont notamment le référentiel général de gestion des archives.

48 « Délibération 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel », legifrance.gouv.fr

49 « Préserver les données numériques : de quoi parle t-on ? », francearchives.gouv.fr

50 « Les durées de conservation des données », cnil.fr

51 « Publications et ressources », gouvernement.fr

FICHE 12 - ENCADRER LES DÉVELOPPEMENTS INFORMATIQUES

Intégrer sécurité et protection des données personnelles au plus tôt dans les projets.

La protection des données personnelles doit être intégrée dans le cycle de développement informatique dès la phase de conception et pour les configurations par défaut afin d'offrir aux personnes concernées une meilleure maîtrise de leurs données et de limiter les erreurs, pertes, modifications non autorisées, ou mauvais usages de celles-ci dans les applications.

Les précautions élémentaires

- **Intégrer la protection des données, y compris ses exigences en termes de sécurité des données, dès la conception** de l'application ou du service. Ces exigences peuvent se traduire par divers choix d'architecture (décentralisée ou centralisée), de fonctionnalités (ex. : anonymisation à bref délai, minimisation des données), de technologies (ex. : chiffrement des communications), etc.
- **Mettre en place une défense en profondeur** des systèmes (combinaison de plusieurs mesures de sécurité).
- **Pour tout développement à destination du grand public, mener une réflexion sur les paramètres influant sur le respect de la vie privée,** et notamment sur le paramétrage par défaut.
- **Éviter le recours à des zones de texte libre ou de commentaire**, sources de collecte de données personnelles supplémentaires non nécessaires ou disproportionnées.
- **Réaliser des tests complets (unitaires, d'intégration et fonctionnels)** avant la mise à disposition ou la mise à jour d'un produit.
- Effectuer les développements informatiques et les tests dans un environnement informatique distinct de celui de la production (ex. : sur des ordinateurs ou des machines virtuelles différents) et sur des données fictives ou anonymisées.
- **Effectuer un audit ou une revue de code avant tout passage en production d'une mise à jour** pour éviter l'apparition de sources de violation de données personnelles.

Ce qu'il ne faut pas faire

- Utiliser des données personnelles 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 ou de protection des données personnelles à mettre en place.
- Faire reposer la protection des données sur une seule ligne de défense. Si cette dernière tombe plus rien ne protège les données.

POUR ALLER PLUS LOIN

- La CNIL a publié un **guide RGPD**[52] **spécifiquement à destination des équipes de développement** pour les aider à mettre en conformité leurs développements informatiques avec la règlementation concernant la protection des données personnelles.
- 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 du formulaire.
- Un article dédié aux zones de texte libre ou de commentaires est accessible sur le site de la CNIL[53].
- Les conventions ou règles de codage et la documentation sont essentielles pour maintenir l'application ou le service dans le temps sans introduire de nouvelles vulnérabilités et pour corriger efficacement les dysfonctionnements.
- 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, davantage susceptibles d'être maintenus sur le long terme.
- La création et la gestion de profils utilisateur donnant des droits d'accès aux données variant en fonction des catégories d'utilisateur doivent être intégrées dès la phase de conception.
- Les tests menés sur les données fictives ou anonymisées ne sont parfois pas suffisants pour s'assurer du bon fonctionnement d'un nouveau service ou d'une nouvelle fonctionnalité. Il est alors possible de tester dans un environnement de pré-production avec des données réelles. L'environnement de pré-production doit être configuré et sécurisé au même niveau que l'environnement de production lui-même et le nouveau service ou sa mise à jour doit avoir déjà subi l'ensemble des tests (unitaires, d'intégration et fonctionnels) dans les environnements de développement et de test.
- Selon la nature de l'application, il peut être nécessaire d'assurer son intégrité par le recours à des signatures de code exécutable garantissant qu'il n'a subi aucune altération.

52 « Guide RGPD de l'équipe de développement », linccnil.github.io

53 « Zones bloc note et commentaires : les bons réflexes pour ne pas déraper », cnil.fr

FICHE 13 - ENCADRER LA MAINTENANCE ET LA FIN DE VIE DES MATÉRIELS ET LOGICIELS

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

Les opérations de support doivent être encadrées pour maîtriser 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**.
- **Ouvrir les accès nécessaires** à la télémaintenance **à la demande** du prestataire et pour une durée adaptée à l'intervention et définie à l'avance. Ces accès doivent être refermés à l'issue de cette durée.
- 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.**
- **Ne pas laisser seul un intervenant extérieur**, notamment dans les salles sensibles (ex. : salle serveur).
- **Supprimer de façon sécurisée les données des matériels avant leur mise au rebut, leur envoi en réparation chez 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 (ex. : applications qui ne chiffrent pas les communications).
- Réutiliser, revendre ou jeter des supports ayant contenu des données personnelles sans que les données n'aient été supprimées de façon sécurisée.
- Laisser un accès complet ou permanent aux systèmes pour la télémaintenance.

POUR ALLER PLUS LOIN

- Rédiger et mettre en oeuvre une procédure de suppression sécurisée des données.
- 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[54] à des logiciels de ce type.
- Mettre en place des outils de surveillance en temps réel (ex. : sessions « 4 yeux ») ou a posteriori (ex. : enregistrement) des interventions de télémaintenance par des tiers[55].

54 « Produits certifiés CSPN », ssi.gouv.fr

55 Tout comme les systèmes de journalisation, de tels dispositifs doivent être mis en place dans le respect des dispositions légales applicables et en informant les personnes concernées.

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 ne pourra intervenir qu'après autorisation d'accès délivrée par X. L'accès devra être fermé au terme de chaque intervention de Y.

[*Formulation alternative selon la nature de la maintenance :*

En cas de télémaintenance permettant l'accès à distance aux fichiers de X, Y ne pourra intervenir qu'après information délivrée à X, permettant à ce dernier d'identifier et de surveiller les accès à son système d'information.

]

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.

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

FICHE 14 - GÉRER LA SOUS-TRAITANCE

Encadrer la sécurité des données avec les sous-traitants.

Les traitements de données réalisés par un sous-traitant pour le compte du responsable de traitement doivent bénéficier de garanties suffisantes, notamment en matière de sécurité. Le responsable de traitement doit avoir connaissance du détail des mesures de sécurité mises en œuvre par ses sous-traitents est nécessaire pour la démonstration de la conformité[56].

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 et de ses éventuelles certifications.
- **Prévoir un contrat avec les sous-traitants**[57], qui définit notamment l'objet, la durée, la finalité du traitement ainsi que les obligations des parties, notamment en termes de sécurité des traitements. S'assurer qu'il contient en particulier des dispositions fixant :
  - la répartition des responsabilités et des obligations en matière de **confidentialité des données personnelles** confiées ;
  - des **contraintes minimales en matière d'authentification** des utilisateurs ;
  - **les conditions de restitution et 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 et cela dans les plus brefs délais lorsqu'il s'agit d'une violation de données personnelles[58] ;
  - l'assistance que doit fournir le sous-traitant pour garantir le respect des obligations de sécurité[59] ;
  - la revue régulière des mesures de sécurité et, le cas échéant, les conditions de leur révision.
- **Prévoir les moyens permettant de vérifier l'effectivité des garanties offertes par le sous-traitant** en matière de protection des données (ex. : audits de sécurité, visite des installations). 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, mise en place de VPN) ;
  - des garanties en matière de protection du réseau, de traçabilité, de gestion des habilitations, d'authentification, d'audits, etc.

56 Articles 5.2 et 24.1 du RGPD.

57 La Commission européenne a publié des clauses contractuelles types sur lesquelles ce contrat peut reposer (voir : « Clauses contractuelles types entre responsable de traitement et sous-traitant », cnil.fr).

58 Un incident de sécurité est caractérisé de « violation de données à caractère personnel » lorsqu'il touche à des données personnelles.

59 Se référer à l'article 32 du RGPD et au §41 des lignes directrices 07/2020 adoptées par le Comité européen à la protection des données (CEPD).

Ce qu'il ne faut pas faire

- Entamer la prestation de sous-traitance sans avoir signé avec le prestataire un contrat reprenant les exigences posées par l'article 28 du RGPD.
- 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

- La CNIL a publié un guide à destination des sous-traitants[60].
- Consulter et mettre en œuvre les dispositions de l'article 28 du RGPD.
- Concernant le *cloud computing*, privilégier des sous-traitants adhérant à des codes de conduite[61] et s'assurer que ces codes de conduite contiennent, entre autres, des exigences en matière de sécurité et des précisions sur les obligations règlementaires spécifiques au *cloud*. Voir notamment les codes approuvés par les autorités après avis du Comité européen à la protection des données (CEPD) : CISPE[62] et EU Cloud CoC[63].
- Concernant les données de santé, un hébergeur doit disposer d'une certification d'hébergeur de données de santé (HDS)[64]. L'agence du numérique en santé (ANS) publie la liste des hébergeurs certifiés[65]. À noter que la certification a progressivement remplacé l'agrément HDS depuis 2018 et que certains hébergeurs disposent encore d'un agrément[66] valide.

60 « Règlement européen sur la protection des données : un guide pour accompagner les sous-traitants », cnil.fr
61 Article 40 du RGPD.
62 « La CNIL approuve le premier code de conduite européen dédié aux fournisseurs de services d'infrastructure cloud (IaaS) », cnil.fr
63 « L'Autorité de protection des données approuve son premier code de conduite européen », autoriteprotectiondonnees.be
64 « HDS - Certification Hébergeur de Données de Santé », esante.gouv.fr
65 « Liste des hébergeurs certifiés », esante.gouv.fr
66 « Liste des hébergeurs agréés », esante.gouv.fr

FICHE 15 - SÉCURISER LES ÉCHANGES AVEC D'AUTRES ORGANISMES

Renforcer la sécurité de toute transmission de données personnelles.

Sans mesure complémentaire, les canaux de transmission de données grand public (ex. : messagerie électronique, messagerie instantanée, plateforme de dépôt de fichiers) **constituent rarement un moyen de communication sûr** pour transmettre des données personnelles. Une simple erreur d'inattention peut conduire des personnes non habilitées à prendre connaissance de données personnelles, ce qui porte atteinte au droit à la vie privée des personnes concernées. En outre, les entités ayant accès aux serveurs par lesquels transite l'information peuvent avoir accès à leur contenu ou à des métadonnées.

Les précautions élémentaires

- **Chiffrer les données avant leur enregistrement sur un support physique à transmettre à un tiers** (ex. : clé USB, disque dur portable, disque optique).
- **Lors d'un envoi via un réseau :**
  - **chiffrer les pièces** sensibles à transmettre. À ce sujet, il convient de se référer aux préconisations de la fiche n°17 – Chiffrer, hacher ou signer ;
  - utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers, par exemple **SFTP** ou **HTTPS**, en utilisant **les versions les plus récentes des protocoles** ;
  - **assurer la confidentialité des secrets** (ex. : clé de chiffrement, mot de passe) en les transmettant via un canal distinct des données protégées (ex. : envoi du fichier chiffré par e-mail et communication du mot de passe par téléphone ou SMS).
- Ouvrir un fichier venant de l'extérieur seulement si l'expéditeur est connu et après soumission à une **analyse antivirus**.
- 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'adresses des fax les numéros des destinataires potentiels (si la fonction existe).

Ce qu'il ne faut pas faire

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

POUR ALLER PLUS LOIN

- Utiliser des algorithmes à clé publique, lorsque les différents acteurs ont mis en place une **infrastructure de gestion de clés publiques** pour garantir la confidentialité et l'intégrité des communications, ainsi que l'authentification de l'émetteur.
- Faire **signer électroniquement les données** par l'émetteur avant leur envoi afin de garantir qu'il est à l'origine de la transmission (voir la fiche n°17 : Chiffrer, hacher ou signer).
- Utiliser un **serveur de dépôt de fichiers temporaires** peut également être approprié. Dans ce cas, s'assurer de :
  - paramétrer une durée limitée de mise à disposition des fichiers ;
  - restreindre l'accès aux fichiers aux seuls destinataires dûment autorisés ;
  - chiffrer les fichiers avant de les déposer sur le service si la solution utilisée ne prévoit pas cette possibilité de manière intégrée.
- Certains outils et solutions de communication protègent aussi les métadonnées liées aux éléments échangés et peuvent être utilisés lorsque celles-ci présentent une sensibilité particulière.
- Pour les systèmes les plus sensibles, cantonner les fichiers venant de l'extérieur à des zones isolées du reste du système pour éviter la propagation de logiciels malveillants.

FICHE 16 - 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 papier ou aux matériels informatiques, notamment aux serveurs. Les locaux doivent également être protégés contre les autres types de menaces (ex. : incendie, inondation).

Les précautions élémentaires

- Installer des **alarmes anti-intrusion** et vérifier leur bon fonctionnement 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 ainsi que les codes d'alarme.
- **Distinguer les zones des bâtiments selon les risques** (ex. : 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 et faire une revue périodique de cette liste.
- **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**[67] par une personne appartenant à l'organisme.
- Protéger l'accès au réseau (ex. : prises dans les bureaux, baies de brassage) et ne permettre qu'aux équipements autorisés de s'y connecter.
- Protéger physiquement les matériels informatiques par des moyens spécifiques (ex. : système anti-incendie dédié, surélévation contre d'éventuelles inondations, redondance d'alimentation électrique, redondance de système de climatisation).

Ce qu'il ne faut pas faire

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

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

POUR ALLER PLUS LOIN

- Conserver une trace des accès aux salles ou bureaux susceptibles de contenir du matériel traitant des données personnelles pouvant avoir un impact négatif grave sur les personnes concernées en cas d'incident. **Informer les utilisateurs** de la mise en place d'un tel système, après information et consultation des instances représentatives du personnel.
- S'assurer que seul le personnel dûment habilité soit admis dans les zones à accès restreint. Par exemple :
  - à l'intérieur des zones à accès règlementé, exiger l**e port d'un moyen d'identification visible** (ex. : badge) pour toutes les personnes ;
  - les visiteurs (ex. : personnel en charge de l'assistance technique) ne doivent avoir qu'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.

FICHE 17 - CHIFFRER, HACHER 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'authenticité du signataire et d'assurer la non-répudiation. 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-2[68] ou SHA-3[69] comme familles de fonctions de hachage ;
  - HMAC utilisant SHA-2 ou SHA-3, bcrypt, scrypt, Argon2 ou PBKDF2 pour stocker les mots de passe ;
  - AES[70] avec un mode de construction approprié (CCM, GCM, ou EAX) ou ChaCha20[71] (avec Poly1305) pour le chiffrement symétrique ;
  - RSA-OAEP[72], ECIES-KEM[73] ou DLIES-KEM[73] pour le chiffrement asymétrique ;
  - RSA-SSA-PSS[72] pour les signatures.
- **Utiliser des tailles de clés suffisantes** :
  - pour AES, il est recommandé d'utiliser des clés de 128 bits a minima ;
  - pour les algorithmes basés sur RSA, il est recommandé d'utiliser des modules et exposants secrets d'au moins 2 048 bits ou 3 072 bits, avec des exposants publics, pour le chiffrement, supérieurs à 65 536 bits.
- **Appliquer les recommandations d'utilisation appropriées**, en fonction de l'algorithme utilisé. Les erreurs d'implémentation ont un impact important sur la sécurité du mécanisme cryptographique.
- **Protéger les clés secrètes,** a minima 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 du mot de passe de déverrouillage.

68 Comme défini dans le standard NIST FIPS 180-4.

69 Comme défini dans le NIST FIPS 202.

70 Comme défini dans le NIST FIPS 197.

71 Comme défini dans la RFC 8439.

72 Comme défini dans le standard RSA PKCS#1 v2.2.

73 Comme définis dans la norme ISO/IEC 18033-2.

Ce qu'il ne faut pas faire

- Utiliser des algorithmes obsolètes, comme les chiffrements DES et 3DES ou les fonctions de hachage MD5 et SHA-1.
- Confondre fonction de hachage et de 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 l'exécution, il est souvent possible de tester automatiquement toutes les possibilités et ainsi de reconnaître l'empreinte.

POUR ALLER PLUS LOIN

- Voir la page dédiée « *Comprendre les grands principes de la cryptologie et du chiffrement* » sur le site de la CNIL[74].
- L'ANSSI a publié des **guides**[75] pour aider **les développeurs et administrateurs dans leurs choix d'algorithmes cryptographiques, de dimensionnement et d'implémentation**.
- 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, telles que :
  - les solutions certifiées ou qualifiées par l'ANSSI[76] ;
  - le logiciel VeraCrypt, permettant la mise en œuvre de conteneurs[77] chiffrés ;
  - le logiciel GNU Privacy Guard, permettant la mise en œuvre de la cryptographie asymétrique (signature et chiffrement)[78].
- Pour les autorités administratives, les annexes du référentiel général de sécurité (RGS)[79] s'appliquent, notamment les annexes B1 et B2 concernant respectivement les mécanismes cryptographiques et la gestion des clés utilisées.

74 « Comprendre les grands principes de la cryptologie et du chiffrement », cnil.fr
75 « Mécanismes cryptographiques », ssi.gouv.fr
76 « Visa de sécurité », ssi.gouv.fr
77 Par conteneur, il faut comprendre un fichier susceptible de contenir plusieurs autres fichiers.
78 « The Gnu Privacy Guard », gnupg.org
79 « Liste des documents constitutifs du RGS v.2.0 », ssi.gouv.fr

ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE VOTRE ORGANISME

Avez-vous pensé à ... ?

FICHES		MESURES	
1	**Sensibiliser les utilisateurs**	Informer et sensibiliser les personnes manipulant les données	☐
		Rédiger une charte informatique et lui donner une force contraignante	☐
2	**Authentifier les utilisateurs**	Définir un identifiant (« *login* ») unique pour chaque utilisateur	☐
		Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL	☐
		Obliger l'utilisateur à changer le mot de passe attribué automatiquement ou par un administrateur	☐
		Limiter le nombre de tentatives d'accès à un compte	☐
3	**Gérer les habilitations**	Définir des profils d'habilitation	☐
		Supprimer les permissions d'accès obsolètes	☐
		Réaliser une revue annuelle des habilitations	☐
4	**Tracer les opérations et gérer les incidents**	Prévoir un système de journalisation	☐
		Informer les utilisateurs de la mise en place du système de journalisation	☐
		Protéger les équipements de journalisation et les informations journalisées	☐
		Prévoir les procédures et les responsabilités internes pour la gestion des incidents, dont la procédure de notification aux régulateurs des violations de données personnelles	☐
5	**Sécuriser les postes de travail**	Prévoir une procédure de verrouillage automatique de session	☐
		Utiliser des antivirus régulièrement mis à jour	☐
		Installer un pare-feu (« *firewall* ») logiciel	☐
		Recueillir l'accord de l'utilisateur avant toute intervention sur son poste	☐
6	**Sécuriser l'informatique mobile**	Prévoir des moyens de chiffrement des équipements mobiles	☐
		Faire des sauvegardes ou des synchronisations régulières des données	☐
		Exiger un secret pour le déverrouillage des smartphones	☐
7	**Protéger le réseau informatique interne**	Limiter les flux réseau au strict nécessaire	☐
		Sécuriser les accès distants des appareils informatiques nomades par VPN	☐
		Sécuriser ses réseaux Wi-Fi, notamment en mettant en œuvre le protocole WPA3	☐
8	**Sécuriser les serveurs**	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées	☐
		Installer sans délai les mises à jour critiques	☐
		Assurer une disponibilité des données	☐

FICHES		MESURES	
9	**Sécuriser les sites web**	Utiliser le protocole TLS et vérifier sa mise en œuvre	☐
		Vérifier qu'aucun mot de passe ou donnée personnelle ne passe par les URL	☐
		Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu	☐
		Mettre un bandeau de consentement pour les *cookies* non nécessaires au service	☐
10	**Sauvegarder et prévoir la continuité d'activité**	Effectuer des sauvegardes régulières	☐
		Stocker les supports de sauvegarde dans un endroit sûr	☐
		Protéger les sauvegardes, notamment durant leur convoyage	☐
		Prévoir et tester régulièrement la continuité d'activité	☐
11	**Archiver de manière sécurisée**	Mettre en œuvre des modalités d'accès spécifiques aux données archivées	☐
		Détruire les archives obsolètes de manière sécurisée	☐
12	**Encadrer les développements informatiques**	Prendre en compte la protection des données personnelles dès la conception	☐
		Proposer des paramètres respectueux de la vie privée par défaut	☐
		Éviter les zones de commentaires ou les encadrer strictement	☐
		Utiliser des données fictives ou anonymisées pour le développement et les tests	☐
13	**Encadrer la maintenance et la fin de vie des matériels et des logiciels**	Enregistrer les interventions de maintenance dans une main courante	☐
		Encadrer les interventions de tiers par un responsable de l'organisme	☐
		Effacer les données de tout matériel avant sa mise au rebut	☐
14	**Gérer la sous-traitance**	Prévoir des clauses spécifiques dans les contrats des sous-traitants	☐
		Prévoir les conditions de restitution et de destruction des données	☐
		S'assurer de l'effectivité des garanties prévues (ex. : audits de sécurité, visites)	☐
15	**Sécuriser les échanges avec d'autres organismes**	Chiffrer les données avant leur envoi	☐
		S'assurer qu'il s'agit du bon destinataire	☐
		Transmettre le secret lors d'un envoi distinct et via un canal différent	☐
16	**Protéger les locaux**	Restreindre les accès aux locaux au moyen de portes verrouillées	☐
		Installer des alarmes anti-intrusion et les vérifier périodiquement	☐
17	**Chiffrer, hacher ou signer**	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues et sécurisées	☐
		Conserver les secrets et les clés cryptographiques de manière sécurisée	☐

Commission nationale de l'informatique et des libertés
3, Place de Fontenoy - TSA 80715
75334 PARIS CEDEX 07
01 53 73 22 22

Mars 2023

www.cnil.fr
linc.cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS