CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

Les fondamentaux de la sécurité des traitements de données personnelles

Thibaud ANTIGNAC, Ingénieur expert
Anaëlle MORIN, Ingénieure experte

Plan


CNIL.
CONTEXTE
20/06/2023
Webinaire - Les fondamentaux de la sécurité des traitements de données personnelles
3

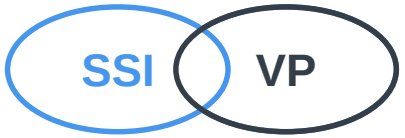

CNIL.
Guide pratique RGPD – Sécurité des données personnelles
MISE A JOUR 2023
20/06/2023
Webinaire - Les fondamentaux de la sécurité des traitements de données personnelles
8


CNIL.
Exemples de mesures pour se protéger d'un rançongiciel
CAS PRATIQUE
20/06/2023
Webinaire - Les fondamentaux de la sécurité des traitements de données personnelles
18


CNIL.
QUESTIONS ?
20/06/2023
Webinaire - Les fondamentaux de la sécurité des traitements de données personnelles
31

CONTEXTE

SSI vs Vie privée



Sécurité des systèmes d'information

Objectif : protéger l'organisme

Sujet de l'étude :

- Les informations manipulées au sein de l'organisme (dont les données à caractère personnel)
- Les processus métiers

Impacts étudiés :

- sur l'image, juridiques (dont le non respect de la Loi Informatique & libertés), financiers…

Protection de la vie privée

Objectif : protéger les personnes concernées et leurs droits

Sujet de l'étude :

- Les données à caractère personnel confiées à l'organisme
- Les processus légaux

Impacts étudiés :

- sur la vie privée, l'identité humaine, les libertés publiques…

La sécurité au cas par cas

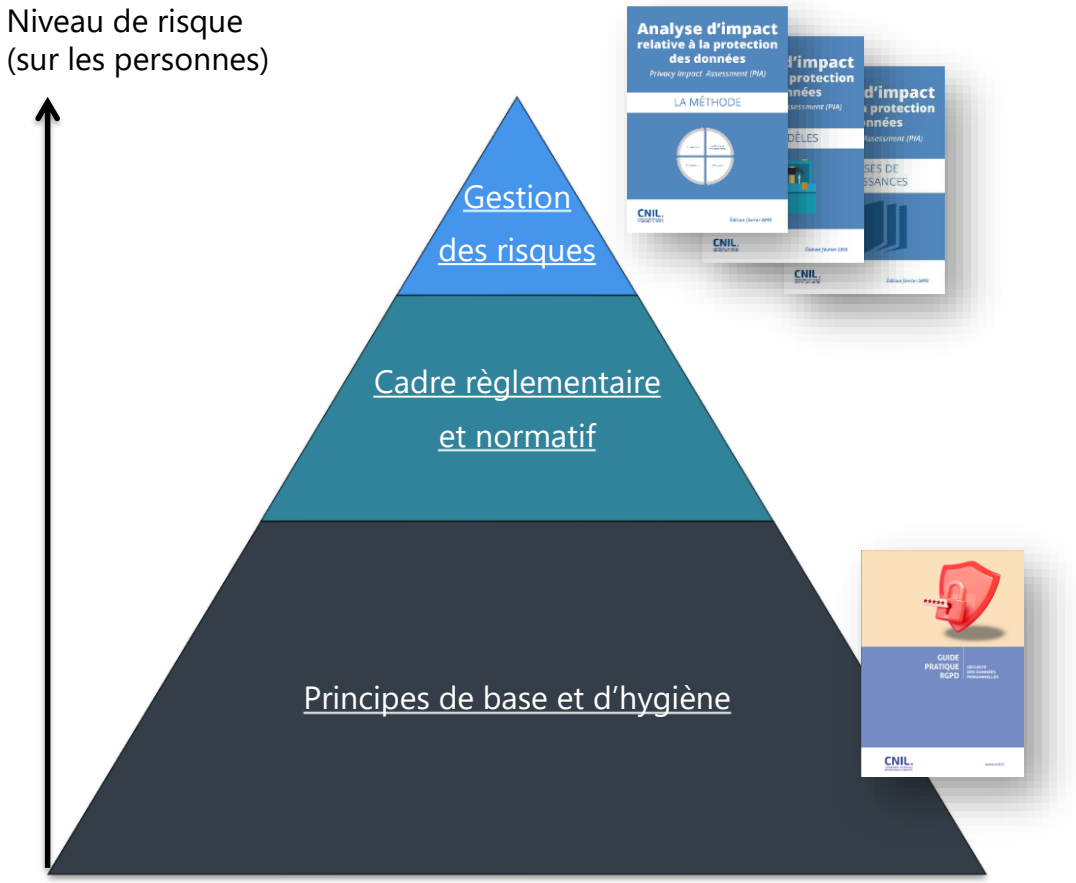
Liste de diffusion

- Nom (ou pseudo), email
- Données à caractère personnel identifiantes
- Conséquences limitées en cas de diffusion, modification ou suppression
- Confidentialité, intégrité, authentification et traçabilité des destinataires nécessaires à un niveau d'assurance « moyen »

Dossiers médicaux numériques

- Données de santé
- Données à caractère personnel identifiantes ET sensibles
- Conséquences graves en cas de diffusion, modification ou suppression
- Confidentialité, intégrité, authentification et traçabilité des destinataires nécessaires à un niveau d'assurance « très élevé »

Logique générale du « niveau approprié »



3. Enfin, les risques devraient être étudiés en détail sur les traitements susceptibles d'engendrer des risques élevés
- Exemples d'outils : Guides et logiciel PIA

2. Ensuite, le cadre règlementaire et normatif (règlements, normes, *etc.*) doit être mis en œuvre
- Exemples d'outils :
  - Ordonnance 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (« RGS »)
  - ISO/IEC 27701:2019 Management de la protection de la vie privée

1. En premier lieu, les principes de base et d'hygiène doivent être mis en place de manière systématique
- Exemple d'outils :
  - Guide pratique RGPD « Sécurité des données personnelles »

Les violations en France en 2022

- **> 4000** notifications de violations
  (> 5000 en 2021)

- **92%** des notifications concernent une **perte de confidentialité**
- **63%** des notifications concernent une **attaque externe**
- **30%** des notifications concernent une attaque par **rançongiciel**

- **Professionnalisation et spécialisation de la sphère criminelle**
  - Crime organisé déterminant avec précision ses cibles
  - Recherche d'accès discrets et pérennes aux réseaux de leurs victimes

Guide pratique RGPD – Sécurité des données personnelles

MISE A JOUR 2023

Contenu du guide

1. Sensibiliser les utilisateurs
2. Authentifier les utilisateurs
3. Gérer les habilitations
4. Tracer les opérations et gérer les incidents
5. Sécuriser les postes de travail
6. Sécuriser l'informatique mobile
7. Protéger le réseau informatique interne
8. Sécuriser les serveurs
9. Sécuriser les sites web
10. Sauvegarder et prévoir la continuité d'activité
11. Archiver de manière sécurisée
12. Encadrer les développements informatiques
13. Encadrer la maintenance et la fin de vie des matériels et logiciels
14. Gérer la sous-traitance
15. Sécuriser les échanges avec d'autres organismes
16. Protéger les locaux
17. Chiffrer, hacher ou signer

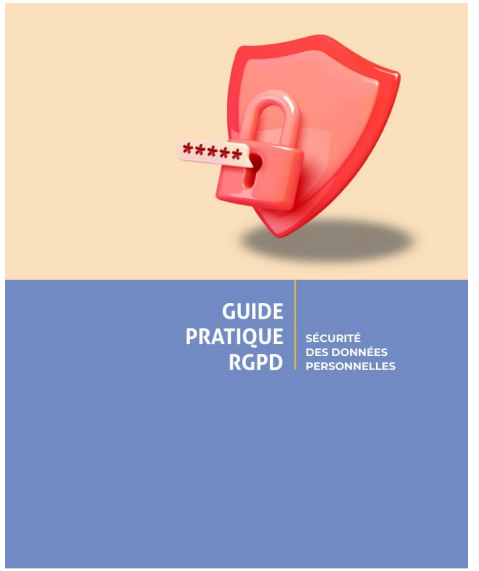
Utilisateurs

Informatique interne

Extérieurs à l'organisme

Sécurité physique

Outils cryptographiques



Fiche 2 : Authentifier les utilisateurs

- Reconnaître les utilisateurs (identifier et authentifier) pour pouvoir, ensuite :
  - Leur donner les accès nécessaires (*-> Fiche 3 : Gérer les habilitations*)
  - Enregistrer les opérations faites sur les données (*-> Fiche 4 : Tracer les opérations et gérer les incidents*)

Changements depuis la version précédente

Fiche 2 : Authentifier les utilisateurs

- Prise en compte de la nouvelle recommandation sur les mots de passe publiée par la CNIL en 2022 :
  - ~~Renouvellement automatique des mots de passe~~ (sauf pour les administrateurs)
  - On parle dorénavant d'entropie
- L'utilisation des gestionnaires de mots de passe devient recommandée dès les précautions élémentaires
- Évolution du stockage des mots de passe :
  - ~~Fonction de hachage cryptographique (HMAC utilisant SHA-256)~~
  - Uniquement fonction spécifiquement conçue à cette fin (bcrypt, scrypt, Argon2 ou PBKDF2) *–> Voir fiche 17 : Chiffrer, hacher ou signer*

Fiche 2 : Entropie

	Exemple	*Longueur minimum*	*Composition*	Entropie minimum	Composition
Mot de passe seul	Forum, blog	*12*	*4 types*	80	**12** A-Z,a-z,0-9, %$... **14** A-Z, a-z, 0-9 **7** mots etc.
Avec restriction d'accès (le + répandu)	Sites de e-commerce, compte d'entreprise, webmail	*8*	*3 des 4 types*	50	**8** A-Z,a-z,0-9, %$... **5** mots **16** 0-9 etc.
Avec information complémentaire	Banque en ligne	*5*	*Chiffres et/ou lettres*	**Le mot de passe :** 27 **L'information :** 23	**Le mot de passe :** **8** 0-9 **7** 0-F (0-9 A-F) **L'information :** **7** 0-9 **6** 0-F (0-9 A-F)
Pour matériel détenu par la personne	CB ou téléphone	*4*	*Chiffres*	13	**4** 0-9

Fiche 2 : Authentifier les utilisateurs

- **Pour aller plus loin**
  - **Privilégier l'authentification multifacteur**
  - **Imposer techniquement les règles relatives aux mots de passe et à l'authentification**

- **Ressources**
  - **Recommandation CNIL**
    https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite
  - **Recommandations ANSSI**

    https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/
    https://www.ssi.gouv.fr/guide/mecanismes-cryptographiques

Fiche 4 : Tracer les opérations et gérer les incidents

- Identifier un **accès frauduleux** ou une **utilisation abusive** de données personnelles
- Déterminer l'**origine** et le **déroulé** d'un incident
- Remplir les obligations de **notification en cas de violation**

Changements depuis la version précédente

Fiche 4 : Tracer les opérations et gérer les incidents

- Prévoir un système de journalisation couvrant les événements **métiers, techniques et d'administration**
- Conserver les événements sur une période glissante comprise **entre 6 mois et 1 an**
- Enregistrer :
  - Les opérations de **création**, **consultation**, **modification** et **suppression**
  - La **nature** de l'opération
  - La **référence des données** concernées et non les données elles-mêmes
- **Protéger** les équipements de journalisation et les informations journalisées contre les **mésusages** et les **écrasements** de données
- S'assurer que les **sous-traitants** sont contractuellement tenus aux mêmes recommandations

Changements depuis la version précédente

Fiche 4 : Tracer les opérations et gérer les incidents

- Etablir des **procédures** concernant la génération des **alertes** et leur **traitement**
- Prévoir un dispositif de remontée des incidents par les **utilisateurs** pour tout évènement suspect
- **Diffuser** à tous les utilisateurs la conduite à tenir et la liste des personnes à contacter
- Tenir un **registre interne** de toutes les violations de données personnelles
- **Notifier**
  - **à la CNIL**, dans les 72 heures, les violations présentant un risque pour les droits et libertés des personnes et
  - **les personnes concernées**, dans les meilleurs délais, en cas de risque élevé pour leurs droits et libertés

Changements depuis la version précédente

Fiche 4 : Tracer les opérations et gérer les incidents

- **Pour aller plus loin**
  - Donner accès et faire participer l'utilisateur à la surveillance
  - Privilégier une surveillance automatique des journaux

- **Ressources**
  - Recommandation CNIL
    https://www.cnil.fr/fr/la-cnil-publie-une-recommandation-relative-aux-mesures-de-journalisation
  - Recommandation ANSSI
    https://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journalisation/
  - Assistance aux victimes de cybermalveillance
    https://www.cybermalveillance.gouv.fr

Exemples de mesures pour se protéger d'un rançongiciel

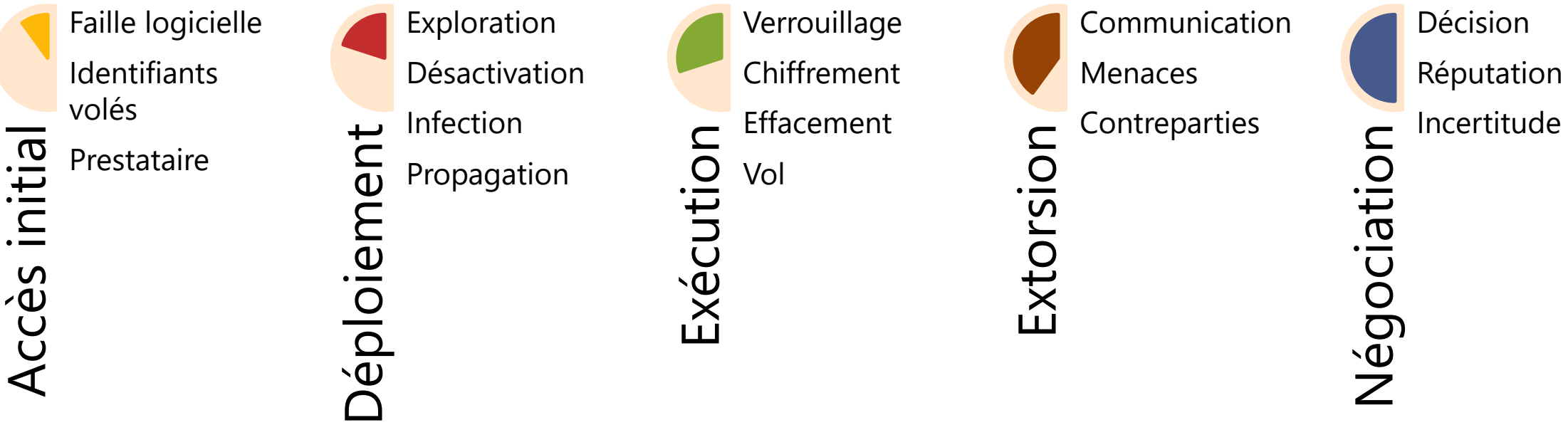
CAS PRATIQUE

Rançongiciels : caractéristiques

Motivations	Cibles
• **Extorsion financière** • Activisme • Espionnage • Sabotage	• **Fichiers** • **Bases de données** • **Ordinateurs** • **Serveurs**

30% des notifications reçues à la CNIL concernent une attaque par **rançongiciel**

Rançongiciels : mode opératoire



ENISA threat landscape for ransomware attacks, July 2022
https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

Fiche 1 : Sensibiliser les utilisateurs

Pourquoi ?

- Nombre important d'utilisateurs du SI
- Utilisateurs aussi bien internes qu'externes
  - Ouverture d'un mail de phishing, erreur de manipulation, mot de passe faible, …

Comment ?

- Sensibiliser les utilisateurs du SI sur les risques et les bonnes pratiques
- Documenter les procédures pour accompagner l'usage
- Imposer une charte informatique pour encadrer l'usage

Fiche 4 : Tracer les opérations et gérer les incidents

Pourquoi ?

- Complexité croissante des attaques et de leurs origines
- Réactions inadaptées et ralenties en l'absence de préparation
- Indispensable pour comprendre les causes d'un incident et empêcher sa réapparition

Comment ?

- Enregistrer les opérations effectuées par tous types d'utilisateurs sur le SI
- Protéger les journaux afin qu'ils ne soient pas touchés par le rançongiciel
- Diffuser les actions immédiates à mettre en œuvre par les utilisateurs
- Identifier les points de contact du responsable de traitement
- Notifier l'incident à la CNIL

Fiche 5 : Sécuriser les postes de travail

Pourquoi ?

- Autant de points d'entrée que d'utilisateurs
- Passerelle avec Internet (navigation, installation de logiciels, boite mail)

Comment ?

- Limiter les droits et les logiciels installés
- Configurer un antivirus et un pare-feu logiciel
- Mettre à jour !

Fiche 6 : Sécuriser l'informatique mobile

Pourquoi ?

- Surface d'attaque supplémentaire et croissante
- Équipements moins bien maitrisés par la DSI
- Nouvelles attaques ciblant directement les équipements mobiles

Comment ?

- Sensibiliser les utilisateurs aux risques spécifiques de leur équipement mobile
- Mettre en place des mesures de sauvegarde des postes nomades
- Limiter le stockage d'informations sensibles sur les postes nomades

Fiche 7 : Protéger le réseau informatique interne

Pourquoi ?

- Interconnecte l'ensemble des composants du SI
- Vecteur de propagation de l'attaque (intrusion, logiciel malveillant) à l'ensemble du SI de l'organisme par sa colonne vertébrale

Comment ?

- Limiter les accès Internet
- Limiter les flux réseau au strict nécessaire (pare-feux)
- Imposer un VPN pour l'accès à distance
- S'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet

Fiche 8 : Sécuriser les serveurs

Pourquoi ?

- Emplacements de stockage des données personnelles
- Cœur des opérations de traitement

Comment ?

- Désactiver et désinstaller les services et interfaces inutiles
- Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
- Adopter une politique spécifique d'authentification pour les administrateurs
- Utiliser des outils de détection et suppression de programmes malveillants
- Installer les mises à jour critiques et de sécurité sans délai

Fiche 10 : Sauvegarder et prévoir la continuité d'activité

Pourquoi ?

- Impossibilité de se prémunir des menaces de manière certaine
  - Capacité d'assurer une partie de l'activité en mode dégradé
  - Capacité de se relever plus rapidement et à moindres coûts

Comment ?

- Sauvegarder fréquemment les données
- Protéger les données sauvegardées au même niveau de sécurité que celles d'exploitation
- Isoler au moins une sauvegarde hors ligne, déconnectée du réseau de l'organisme
- Préparer les plans de continuité (PCA) et de reprise d'activité (PRA) en amont
- Tester régulièrement la restauration des sauvegardes et les PCA et PRA

Fiche 14 : Gérer la sous-traitance

Pourquoi ?

- Ouverture du SI à des personnes extérieures
- Différence de pratiques de sécurité et de niveau de maturité
- Existence d'attaques indirectes passant par les prestataires

Comment ?

- Vérifier la documentation des prestataires (connaissances, ressources, PSSI, certifications)
- Encadrer contractuellement les obligations de chaque partie
- Vérifier l'effectivité des garanties et le respect des engagements par les sous-traitants
- Privilégier les sous-traitants de *cloud computing* adhérant à des codes de conduite (par exemple CISPE et EU Cloud CoC)

Fiche 15 : Sécuriser les échanges avec d'autres organismes

Pourquoi ?

- Absence de sécurisation par défaut de nombreux outils de communication
- La messagerie électronique est le point d'entrée de nombreuses attaques

Comment ?

- Ouvrir un fichier venant de l'extérieur seulement si l'expéditeur est connu et après soumission à une analyse antivirus
- Utiliser des services de filtrage de mails
- Utiliser un antivirus adapté

GUIDE PRATIQUE RGPD

SÉCURITÉ DES DONNÉES PERSONNELLES

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

www.cnil.fr

ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE VOTRE ORGANISME

https://www.cnil.fr/fr/la-cnil-publie-une-nouvelle-version-de-son-guide-de-la-securite-des-donnees-personnelles

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	☐

CNIL. CNIL.

QUESTIONS ?