TOUS CYBER VIGILANTS

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

JOURNÉE DE LA CYBERSÉCURITÉ

10 Avril 2025

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Introduction de la journée

Denis ROBIN

Directeur Général de l'ARS Île-de-France

Naïma MEZAOUR

Directrice du GIP SESAN

TOUS CYBER VIGILANTS

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

JOURNÉE DE LA CYBERSÉCURITÉ

10 Avril 2025

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Conférence Institutionnelle (NIS2/CaRE)

Laure HELENE-DUHESME
Coordinatrice sectorielle santé – ANSSI

Christophe MATTLER
Directeur de projets – DNS

Steven GARNIER
Directeur du domaine cybersécurité – ANS

TOUS CYBER VIGILANTS

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

JOURNÉE DE LA CYBERSÉCURITÉ

10 Avril 2025

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Pause café et visite des stands

TOUS CYBER VIGILANTS

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

JOURNÉE DE LA CYBERSÉCURITÉ

10 Avril 2025

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Quelle place a l'humain dans la gestion de crise ?

Matthieu LANGLOIS
Médecin Anesthésiste réanimateur
Ex-médecin chef du RAID - Enseignant chercheur à ESSEC

TOUS CYBER VIGILANTS

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

JOURNÉE DE LA CYBERSÉCURITÉ

10 Avril 2025

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Structures de Coordination : RGPD & Cybersécurité – *On passe à l'action !*

Valérie CORNU
Directrice – CPTS 78 Nord

Sara BOULIL
Cheffe de projet eSanté – DAC 92 Nord

Emilie SAINZ
Adjointe du Directeur du Département SSI – GIP SESAN

TOUS CYBER VIGILANTS
sesan Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité
ars Agence Régionale de Santé Île-de-France

Structures de Coordination : RGPD & Cybersécurité – *On passe à l'action !*

Valérie CORNU
Directrice
CPTS 78 Nord Porte de Normandie

TOUS CYBER VIGILANTS

CPTS 78 Nord Porte de Normandie

sesan Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

CPTS 78 NORD PORTE DE NORMANDIE & SESAN

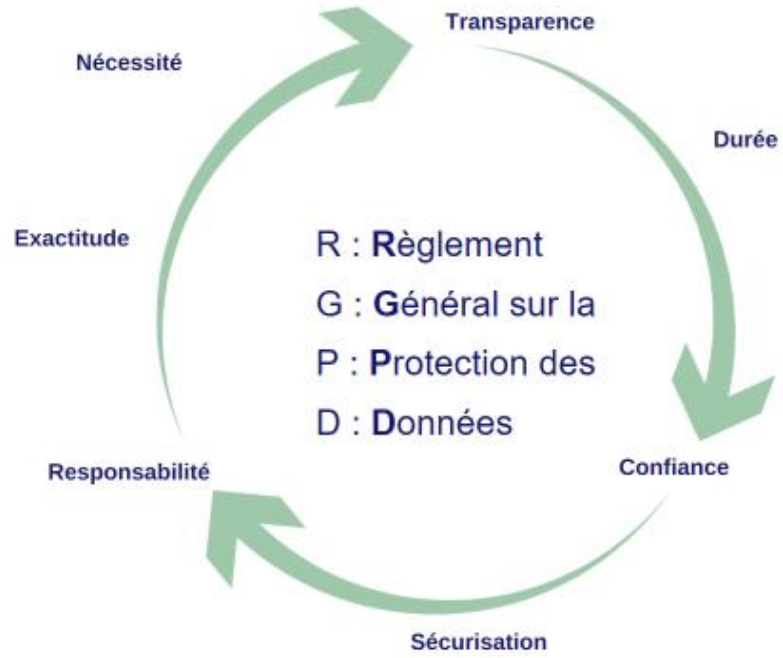
CPTS 78 Nord Porte de Normandie

- Association Loi 1901 - 2020 — ACI 2021 - Taille 3 – Territoire Nord Ouest des Yvelines (57 communes) - Présidente : Dr Gandon Céline - CA Pluri Professionnel — Equipe de coordination
- **Missions :** Faciliter l'accès aux soins (SNP et MT) - Améliorer le parcours des patients pour renforcer la prise en charge – Liens V/H/V - Favoriser le maintien à domicile des patients fragiles - Initier et mettre en place des actions de prévention - Participer à la réponse aux crises sanitaires (Plan SSE Soins de ville) - Améliorer les conditions d'exercice des professionnels - Actions de formations
- **Adhérente** au GIP SESAN
- Accompagnement par Sesan (expérimentation) & Groupe de travail 2023-2024
- Expérimentation de l'outil
- **Amendement et proposition d'un registre simplifié de la CNIL : Mutualisation**

Pour accompagner les CPTS sur la tenue de leur conformité au règlement

LE RGPD – C'EST QUOI

Le règlement général sur la protection des données (RGPD) responsabilise les organismes publics et privés qui traitent leurs données.



- Ne collecter que les données vraiment nécessaires pour atteindre votre objectif.
- Soyez transparent.
- Organisez et facilitez l'exercice des droits des personnes. .
- Fixez des durées de conservation.
- Sécurisez les données et identifiez les risques.

ALORS ...

► https://www.cnil.fr/fr

LA MISE EN CONFORMITE AU RGPD EST-ELLE OBLIGATOIRE POUR LES CPTS ?

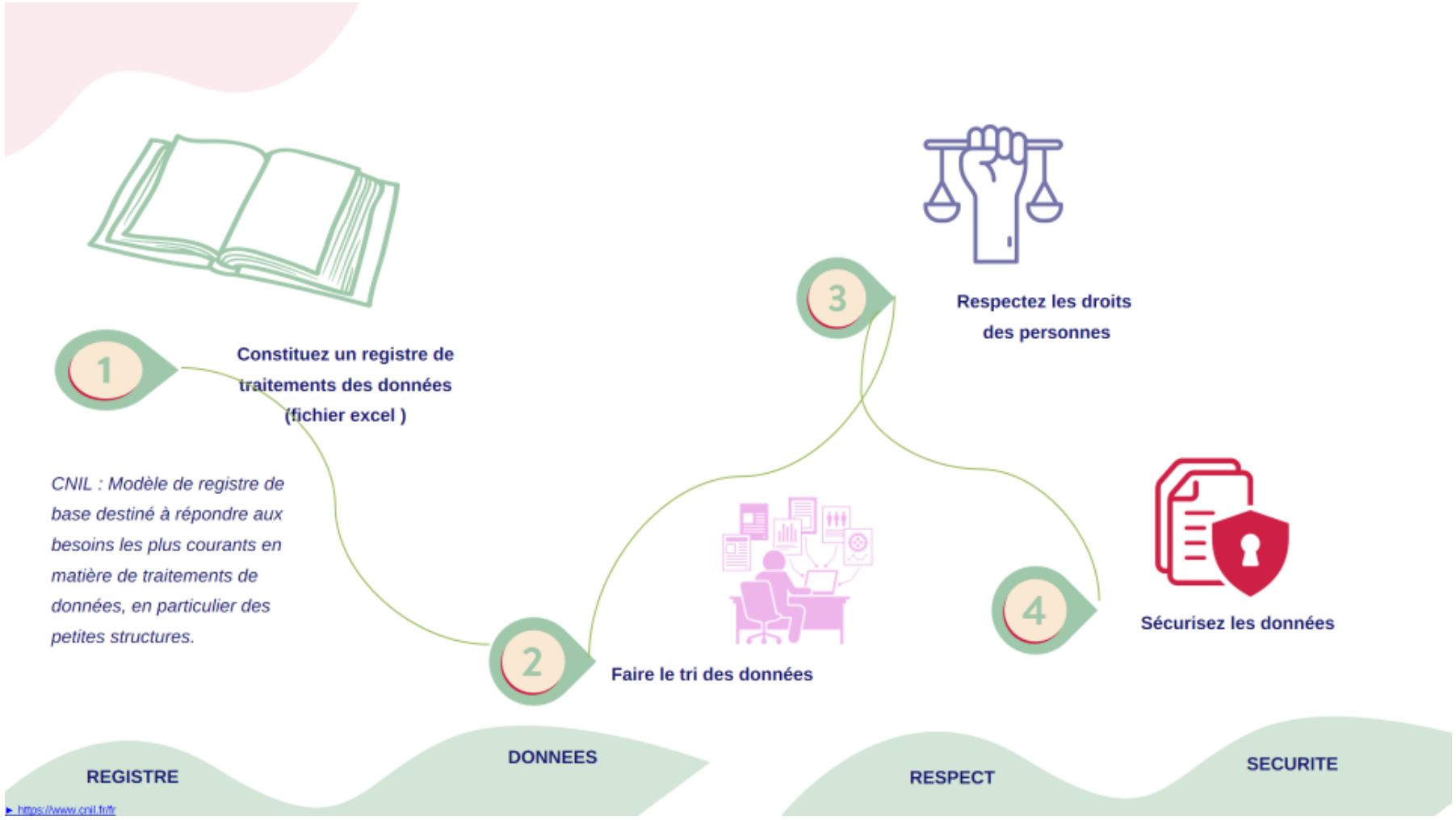
Oui - Pour tous les organismes quelle que soit leur taille, leur secteur d'activité

Ce sont les dirigeants des organismes qui portent la responsabilité de la conformité au RGPD.

Cependant les actions de **conformité peuvent être déléguées (maintien du registre, audit des traitements, rédaction de mentions d'information, mise en œuvre des mesures de sécurité...)**

Attention, la responsabilité juridique ne peut pas être déléguée.

COMMENT FAIRE ?



LE REGISTRE SIMPLIFIÉ POUR LES CPTS

- Vise à recenser les traitements de données personnelles mis en œuvre dans les CPTS en tant que responsable de traitement
- Centralisé et régulièrement mis à jour, il permet de répondre à l'obligation de tenir un registre prévue par le RGPD
- Constitué d'une liste de traitement (onglet 2) et d'au moins une fiche de registre (onglet 3)

Une fiche traitement de données par action (ex : RH, accès MT ….)

Une fois le recensement des traitements effectué,

Etre en mesure d'identifier les actions à mener pour se mettre en conformité

COMPOSITION DU DOCUMENT

Onglet 1 : Tutoriel et questions fréquentes

Onglet 2 "Liste des traitements"

Cet onglet permet de lister toutes les activités des CPTS qui nécessitent de traiter des données personnelles.

Onglet 3 "Modèle de fiche de registre"

Créer et tenir à jour une fiche de registre par activité.

Dupliquer et compléter autant de fois que nécessaire ce modèle de fiche.

Onglet 4 "Exemple de fiche de registre"

Cette partie propose un exemple possible de mise en page et de saisie du registre.

Il est proposé un exemple basé sur un traitement fictif, qu'il ne faut pas reprendre tel quel mais à adapter en fonction de votre traitement.

Onglet 5 : Liste déroulante

EXEMPLE

► Onglet 2 "Liste des traitements"								
Coordonnées du responsable de l'organisme	Nom :		Prénom :		Adresse :		Adresse mail :	
	Code postal :		Ville :		Téléphone :			
Coordonnées du représentant(CPTS non concerné)	Nom :		Prénom :		Adresse :		Adresse mail :	
	Code postal :		Ville :		Téléphone :			
Coordonnées du délégué à la protection des données (DPO) ou personne chargée de la conformité RGPD	Nom :		Prénom :		Société (si DPO externe) :		Adresse :	
	Code postal :		Ville :		Téléphone :		Adresse mél :	
Identification du traitement				Finalité du traitement			Données sensibles ?	
Nom du traitement	N° / RÉF	Date de création de la fiche	Dernière mise à jour de la fiche				Oui/non	
Exemple: Accès medecin traitant	A1-AS-01	26/5/2018	13/5/2019	Mettre en relation les usager avec des professionnels de santé			Oui	
Exemple: Soins non programmés	A1-AS-02	27/5/2024		...			Oui	
Autres exemples de fiches possibles								
ORGANISATION DES PARCOURS	A2-O-01							
ACTIONS DE PREVENTION	A3-P-01							
PARTICIPER A LA REPONSE AUX CRISES SANITAIRES	A4-SS-01							
ATTRACTIVITE DU TERRITOIRE	A5-AT-01							
QUALITE ET DE LA PERTINENCE DES SOINS	A6-Q-01							
MISE A JOUR DU SITE INTERNET DE LA CPTS	ADM-01							
ADHESIONS DES PS	ADM-02							
ANNUAIRE DES PS	ADM-03							
RESSOURCES HUMAINES	ADM-04							
COMPTABILITE /								

DPO & CPTS

Une CPTS peut-elle se mettre en conformité au RGPD sans Délégué à la Protection des données ?

Une CPTS peut se mettre en conformité au RGPD sans DPO en suivant
4 étapes pour entamer et maintenir sa conformité avec les règles de protection des données.

1.
Registre de traitement des données

2.
Faire le tri des données

3.
Respectez les droits des personnes

4.
Sécurisez les données

Avec une fonction située au cœur de la conformité au règlement européen sur la protection des données (RGPD), le délégué à la protection des données (DPO) conseille et accompagne les organismes qui le désignent.

DPO & CPTS

Une CPTS a-t-elle l'obligation d'avoir un DPO ?

Le RGPD prévoit 3 cas où la nomination d'un délégué à la protection des données (DPO) est obligatoire.

Les CPTS pourraient être concernées par un seul cas prévu par le RGPD :

La désignation d'un DPO est obligatoire au titre de l'article 37 point c) **lorsque « les activités de base du responsable du traitement [...] consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 (...). »**

Le Comité Européen de la protection des données donne les exemples suivants dans ses lignes directrices sur le DPO (WP243) :

" **Exemples de traitement à grande échelle: traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités"**

Exemple ne constituant pas un traitement à grande échelle : "traitement, par un médecin exerçant à titre individuel, des données de ses patients« .

Il ne semble pas obligatoire pour les CPTS d'avoir un DPO dans la mesure où le volume de traitement de données sensibles pourrait s'apparenter à celui d'un cabinet de médecin exerçant à titre individuel.

Toutefois si la CPTS souhaite recourir à l'assistance d'un DPO, elle est libre de le faire,

► https://www.cnil.fr/fr

QU'EST CE QU'UNE DONNÉE DE SANTÉ ?

Les informations relatives à une personne physique collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services :

- **Un numéro, un symbole ou un élément spécifique** attribué à une personne physique pour l'identifier de manière unique à des fins de santé.
- **Les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle**, y compris à partir des données génétiques et d'échantillons biologiques.
- **Les informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical** de la personne concernée (indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro).

Exemple: Une information sur une Affection Longue Durée (ALD) est une donnée de santé.

La notion de données de santé est désormais large.

Elle est à apprécier, au cas par cas, compte tenu de la nature des données recueillies.

► https://www.cnil.fr/fr

UNE CPTS A-T-ELLE L'OBLIGATION D'INFORMER LES PERSONNES DU TRAITEMENT DE LEURS DONNÉES PERSONNELLES ?

Oui - À chaque fois que des données personnelles sont collectées, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information sur : l'objectif poursuivi, le fondement juridique, les catégories de personnes qui vont accéder aux données (services, institutions, professionnels,…), le temps de conservation, les modalités d'exercice des droits et recours)

Tout site web doit permettre d'identifier son responsable et son hébergeur, en application de la loi pour la confiance dans l'économie numérique du 21 juin 2004

Si des cookies non nécessaires sur les sites web, il convient de r**ecueillir le consentement de l'internaute après information de celui-ci et avant le dépôt du cookie.**

► https://www.cnil.fr/fr

COMMENT SECURISER LES DONNEES DE LA CPTS ?

Appliquer les règles de sécurité propres à chaque type de traitement de données

Mesures de sécurité techniques (antivirus, accès chiffré, hébergement sécurisé, coffre fort numérique, messagerie sécurisée, maîtrise des flux entrants et sortants …)

Mesures de sécurité organisationnelles (analyse de risques, politique de mot de passe, charte informatique, cartographie du système d'information, clauses de sécurité dans les contrats, gestion des accès au système d'information,…)

Mesures de sécurité physiques (clé, badges …)

Il convient de distinguer les mesures de sécurité appropriées selon le type de traitement (collecte, partage, consultation,…)

Ces mesures permettent de protéger les données contre l'accès non autorisé à de la donnée sensible ou des cyberattaques

(accès au dossier patient, piratage de données, exfiltration de données à des fins non approuvés…).

La CNIL propose un guide "Guide de la sécurité des données personnelles" afin d'aider tous les professionnels à sécuriser les données.

SESAN accompagne les acteurs en santé dans la sécurisation de leurs données : https://cyberservices.sante-idf.fr/

QUE FAIRE EN CAS DE CYBERATTAQUE ?

Le plus rapidement possible

1 - **Débranchez** la machine d'internet et du réseau. Désactivez la connexion Wifi.

2 - **N'éteignez pas** les ordinateurs et matériels affectés par l'attaque pour éviter de supprimer des traces de l'attaque utiles pour les investigations à venir.

3 - **Alertez** au plus vite la hiérarchie et les équipes de la CPTS pour prendre les mesures nécessaires mais également parer une mauvaise manipulation de la part d'un autre collaborateur qui pourrait aggraver la situation

4 - Alertez au plus vite votre support informatique pour prendre les mesures nécessaires pour contenir, voire réduire les conséquences de la cyberattaque

5 - **Déclarez** à la CNIL la cyberattaque en cas de violation de données des personnes et informez les personnes concernées

En cas de rançongiciel, ne payez jamais la rançon demandée

GUIDE ACCOMPAGNEMENT CPTS et RGDP

1 Registre des traitements - Fiche Tutorielle

Pour faciliter la tenue du registre, la CNIL propose un modèle de registre de base destiné à répondre aux besoins les plus courants en matière de traitements de données, en particulier des petites structures.

Ce registre simplifié de la CNIL a été amendé afin d'accompagner les CPTS sur la tenue de leur conformité au Règlement.

Ce document vise à recenser les traitements de données personnelles mis en œuvre dans votre organisme en tant que responsable de traitement.

Centralisé et régulièrement mis à jour, il vous permet de répondre à l'obligation de tenir un registre prévue par le RGPD.

Votre registre sera finalement constitué d'une liste de traitement (onglet 2) et d'au moins une fiche de registre (onglet 3)

► Pour plus d'informations sur les registres de traitement, vous pouvez consulter la page dédiée sur le site de la Cnil.

► Une fois le recensement de vos traitements effectué, vous serez en mesure d'identifier les actions à mener pour vous mettre en conformité.

Dans certains cas, des commentaires seront proposés pour vous aider à compléter votre registre (triangle rouge dans la cellule).

2 Composition du document

► **Onglet 2 "Liste des traitements"**

Cet onglet vous permet de lister toutes les activités de votre CPTS qui nécessitent de traiter des données personnelles.

► **Onglet 3 "Modèle de fiche de registre"**

Vous devez créer et tenir à jour une fiche de registre par activité. Dupliquez et complétez autant de fois que nécessaire ce modèle de fiche.

► **Onglet 4 "Exemple de fiche de registre"**

Cette partie propose un exemple possible de mise en page et de saisie du registre.
Cet exemple est basé sur un traitement fictif, qu'il ne faut pas reprendre tel quel mais à adapter en fonction de votre traitement.

La mise en conformité au RGPD est-elle obligatoire pour les CPTS ?

Oui, pour tous les organismes, quelle que soit leur taille, leur secteur d'activité.

Ce sont les dirigeants des organismes qui portent la responsabilité de la conformité au RGPD.

Cependant les actions de conformité peuvent être déléguées (maintien du registre, audit des traitements, rédaction de mentions d'information, mise en oeuvre des mesures de sécurité...)

Attention, la responsabilité juridique ne peut pas être déléguée.

3 Frise chronologique de la conformité RGPD

Besoin d'aide avec le RGPD ?

► N'hésitez pas à consulter le Guide pratique de sensibilisation au RGPD, disponible sur le site de la CNIL.

Sources

► https://www.cnil.fr/fr

REDACTION DU GUIDE

CPTS 78 Nord Porte de Normandie

sesan Groupement d'Intérêt Public eSanté

V 08 /2024 - Toute reproduction interdite sans autorisation des auteurs

GUIDE ACCOMPAGNEMENT CPTS et RGDP

4 Questions courantes - CPTS

Une CPTS peut-elle se mettre en conformité au RGPD sans DPO ?

Une CPTS peut se mettre en conformité au RGPD sans DPO en suivant 4 étapes pour entamer et maintenir sa conformité avec les règles de protection des données.

Ce document vous aide à valider la première action.
(Cf. : frise chronologique précédente)

Toutefois si la CPTS souhaite recourir à l'assistance d'un DPO, elle est libre de le faire.

Une CPTS a-t-elle l'obligation d'avoir un DPO ?

Il ne semble pas obligatoire pour les CPTS d'avoir un DPO dans la mesure où le volume de traitement de données sensibles pourrait s'apparenter à celui d'un cabinet de médecin exerçant à titre individuel.

Le RGPD prévoit 3 cas où la nomination d'un délégué à la protection des données (DPO) est obligatoire (voir la référence: https://www.cnil.fr/fr/cnil-direct/question/reglement-europeen-le-delegue-la-protection-des-donnees-cest-obligatoire).
Les CPTS pourraient être concernées par un seul cas prévu par le RGPD :
La désignation d'un DPO est obligatoire au titre de l'article 37 point c) lorsque « les activités de base du responsable du traitement [...] consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 (…). »
Le Comité Européen de la protection des données donne les exemples suivants dans ses lignes directrices sur le DPO (WP243) :
" Exemples de traitement à grande échelle: traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités"
Exemples ne constituant pas un traitement à grande échelle:
"traitement, par un médecin exerçant à titre individuel, des données de ses patients"

Qu'est ce qu'une donnée de santé ?

Les informations relatives à une personne physique collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services : un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé.
Les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir des données génétiques et d'échantillons biologiques.
Les informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée (indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro).

Exemple: Une information sur une Affection Longue Durée (ALD) est une donnée de santé.
La notion de données de santé est désormais large.
Elle est à apprécier, au cas par cas, compte tenu de la nature des données recueillies.

Une CPTS a-t-elle l'obligation d'informer les personnes du traitement de leurs données personnelles ?

Oui - À chaque fois que des données personnelles sont collectées, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information sur: l'objectif poursuivi, le fondement juridique, les catégories de personnes qui vont accéder aux données (services, institutions, professionnels,...), le temps de conservation, les modalité d'exercice des droits et recours)

Tout site web doit permettre d'identifier son responsable et son hébergeur, en application de la loi pour la confiance dans l'économie numérique du 21 juin 2004,

Si des cookies non nécessaires sur les sites web, il convient de recueillir le consentement de l'internaute après information de celui-ci et avant le dépôt du cookie.

REDACTION DU GUIDE

V 08 /2024 - Toute reproduction interdite sans autorisation des auteurs

Questions courantes - CPTS

Comment sécuriser les données d'une CPTS ?

Il convient d'appliquer les règles de sécurité propres à chaque type de traitement de données :

- Mesures de sécurité techniques (antivirus, accès chiffré, hébergement sécurisé, coffre fort numérique, messagerie sécurisée, maitrise des flux entrants et sortants ...)
- Mesures de sécurité organisationnelles (analyse de risques, politique de mot de passe, charte informatique, cartographie du système d'information, clauses de sécurité dans les contrats, gestion des accès au système d'information,...)
- Mesures de sécurité physiques (clé, badges ...)

La CNIL propose un guide "Guide de la sécurité des données personnelles" afin d'aider tous les professionnels à sécuriser les données.

Des travaux sont menés également par SESAN pour accompagner les acteurs en santé dans la sécurisation de leurs données : https://cyberservices.sante-idf.fr/

Ces mesures permettent de protéger les données contre l'accès non autorisé à de la donnée sensible ou des cyberattaques (accès au dossier patient, piratage de données, exfiltration de données à des fins non approuvés...).

Il convient de distinguer les mesures de sécurité appropriées selon le type de traitement
(collecte, partage, consultation,...)

Consignes en cas de CYBERATTAQUE

Le plus rapidement possible

1. Débranchez la machine d'internet et du réseau. Désactivez la connexion Wifi.
2. N'éteignez pas les ordinateurs et matériels affectés par l'attaque pour éviter de supprimer des traces de l'attaque utiles pour les investigations à venir.
3. Alertez au plus vite la hiérarchie et les équipes de la CPTS pour prendre les mesures nécessaires mais également parer une mauvaise manipulation de la part d'un autre collaborateur qui pourrait aggraver la situation
Indiquer ci après le ou les contacts :

4. Alertez au plus vite votre support informatique pour prendre les mesures nécessaires pour contenir, voire réduire les conséquences de la cyberattaque
Indiquer ci après le ou les contacts :

5. En cas de rançongiciel, ne payez jamais la rançon demandée

REDACTION DU GUIDE

CPTS Nord Porte de Normandie

sesan Groupement d'Intérêt Public eSanté

Merci

21 chemin des ardilles 78680 EPONE

contact@cpts78nord.fr

06 66 16 78 22

www. cpts78nord.sante-idf.fr

Structures de Coordination : RGPD & Cybersécurité – *On passe à l'action !*

Sara BOULIL
Cheffe de projet eSanté – DAC 92 Nord

sesan Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité
ars Agence Régionale de Santé Île-de-France

Avant l'audit :

CONTEXTE

- Structure de moins de 50 salariés
- Antécédent de cyberattaque par rançongiciel en 2019
- Volonté d'améliorer les pratiques et de se conformer aux nouvelles recommandations

PRÉPARATION

- **Acteurs impliqués** : Direction, Chef de projet (CDP) et service informatique
- **Méthodologie** : Préparation via un questionnaire d'environ 20 questions, élaboré en collaboration avec le service informatique

PROBLÉMATIQUES

- Absence de protocole formalisé en cas de cyberattaque
- Absence de **PCRA** (Plan de Continuité et de Reprise d'Activité)
- Manque de sensibilisation des collaborateurs à la cybersécurité

ATTENTES

- Obtenir un état des lieux de la cybersécurité et une évaluation du niveau de maturité
- Bénéficier d'un regard expert externe sur les pratiques en place

Pendant l'audit :

Déroulement

Durée : 1h30

Mode : Présentiel

Participants : Direction et Chef de projet (CDP)

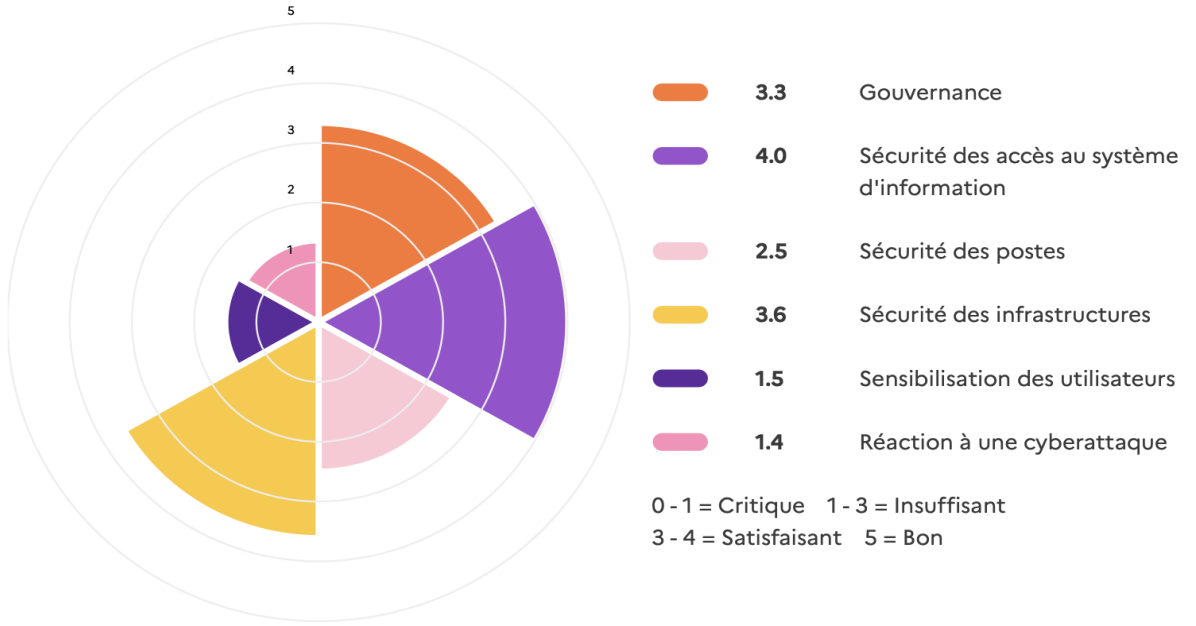
Méthodologie

Format : Questions à choix multiples (QCM) et réponses

Restitution : Envoi immédiat du rapport par e-mail

Suivi

Point d'étape : Réévaluation après 6 mois



Après l'audit :

GOUVERNANCE

- **Réunion CODIR** : Analyse des résultats de l'audit et réflexion sur la stratégie interne
- **Désignation des référents** en cybersécurité au sein de l'organisation
- **Validation du lancement des groupes de travail (GT)** pour l'élaboration d'un **Plan de Continuité et de Reprise d'Activité (PCRA)**
- **Implication active de la DPO** dans le processus
- Prise en compte des enjeux de **sécurité, coût et conformité – un BUDGET CYBER ?**

SENSIBILISATION

- **Flash cyber** en réunion d'équipe (mot de passe, protection des données patients…)
- **Ateliers cybersécurité :** jeux de cartes de plusieurs niveaux
- **Sessions de coaching individuelles** :
  - Création et gestion de mots de passe robustes
  - Importance des mises à jour
  - Sensibilisation au phishing et aux logiciels non officiels
  - Réaction face à une cyberattaque

SECURITÉ

- Mise en place de **l'ERD** et application de la **directive NIS 2**
- Évaluation de la pertinence du serveur interne et analyse des alternatives : migration vers le **cloud** ou acquisition d'un **nouveau serveur**

RÉACTION

- Mise en place d'un **protocole de réponse**, affiché dans tous les bureaux afin que chaque collaborateur sache comment réagir face à une cyberattaque.
- **Début des travaux en mai** pour l'élaboration du **PCRA** en prenant en compte les besoins de chaque entité, avec la participation de plusieurs collaborateurs.

Et malgré tout !

HACKED

Prestataire informatique !

Cette photo par Auteur inconnu est soumise à la licence CC BY-SA-NC

Structures de Coordination : RGPD & Cybersécurité – *On passe à l'action !*

Emilie SAINZ

Adjointe du Directeur du Département SSI – GIP SESAN

SESAN vous accompagne

Une startup d'état

MonAideCyber

INNOVATION ANSSI

MonAideCyber est une start-up d'État incubée au sein du laboratoire d'innovation de l'**Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).**

Pour toutes les entités novices

MonAideCyber s'adresse aux **entités publiques, associatives et privées,** déjà sensibilisées et de **faible maturité cyber**, qui **souhaitent s'engager** dans une démarche **progressive.**

Une démarche concrète

Clé-en-main et **pédagogique**, MonAideCyber rend la cybersécurité accessible à toutes et tous, et facilite la mise en œuvre de **premières mesures** qui réduisent les risques liés à la **cybercriminalité de masse.**

SESAN vous accompagne

https://monaide.cyber.gouv.fr/beneficier-du-dispositif/etre-aide#formulaire-demande-aide

Pour être mis en relation avec l'équipe SSI de SESAN : crrc@sesan.fr

SESAN vous accompagne

L'Aidant cyber va mener avec vous, pendant 1h30, **un diagnostic adapté** aux enjeux cyber actuels.

2

À l'issue du diagnostic, une liste de **6 mesures prioritaires** sont proposées, complétée par **des ressources utiles**.

3

Quelques mois après le diagnostic, **un point d'étape** est organisé pour **vous guider**.

4

Les 6 thématiques abordées :

- La gouvernance
- La sécurité des accès au système d'information
- La sécurité des postes
- La sécurité des infrastructures et des données
- La sensibilisation des utilisateurs
- La réaction à une cyberattaque

SESAN vous accompagne

MonAideCyber
INNOVATION ANSSI

Je suis Aidant

MonAideCyber

crrc@sesan.fr

Venez nous voir sur le Stand SSI

SESAN vous accompagne

Accompagnement RGPD :

- Pilotage RGPD
  - Outil de mise en conformité (Registre, AIPD)
  - Base documentaire

- Sensibilisation (Affiches, campagnes de sensibilisation…)

- Assistance Juridique (Avocat spécialisé dans le droit des technologies de l'information)

- Marché de DPO externe / Assistance au DPO

Venez nous voir sur le Stand SSI

TOUS CYBER VIGILANTS

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

JOURNÉE DE LA CYBERSÉCURITÉ

10 Avril 2025

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

TOUS CYBER VIGILANTS

myCarto

sesan
Île-de-France
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars
Agence Régionale de Santé
Île-de-France

Editeur Français
de **logiciel de cartographie**

+200 organisations cartographient leur SI avec nos solutions

Thibaut DEQUENNE
Directeur commercial

Cédric VOLANDI
Directeur Général

AB SOFTWARE

chm #CHLeMans
GHEF Grand Hôpital de l'Est Francilien
Centre de lutte contre le cancer Léon Bérard
Groupement Hospitalier Portes de Provence
Centre Hospitalier Princesse Grace
CHU Lille
sesan Groupement d'Intérêt Public eSanté
Hôpital Simone Veil Groupement Hospitalier Eaubonne-Montmorency
HUG Hôpitaux Universitaires Genève
Hôpital Paris Saint-Joseph
OPCO Santé
Cerema
Harmonie mutuelle Groupe VYV
université Paris-Saclay
RATP
PARIS
Crédit Agricole
Arts et Métiers ParisTech
Agglo de Saint Quentinois
Auchan
Ministères Territoires Écologie Logement
COLAS
Schmidt Groupe
Région Nouvelle-Aquitaine
FAYAT
UPEC Université Paris-Est Créteil Val de Marne
Finances Publiques
VERSPIEREN Courtier en assurances

“Connaissez-vous bien votre parc informatique et vos actifs métier ?”

* 1ère des 13 recommandations du guide de la CYBERSÉCURITÉ de l’ANSSI

Pourquoi la cartographie doit faire partie de la panoplie du RSSI ?

Sécuriser

Réagir

Auditer

Reconstruire

Cartographie des applications

Dette technique patrimoine IT

Scénarios d'impact

Plan de communication

Plan Continuité d'Activité

Plan Reprise d'Activité

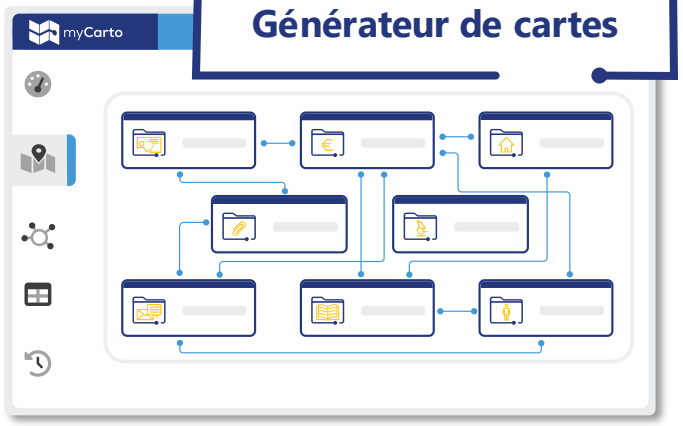
5 couches pour urbaniser votre SI

- Métier
- Data
- Fonctionnelle
- Applicative
- Infrastructure

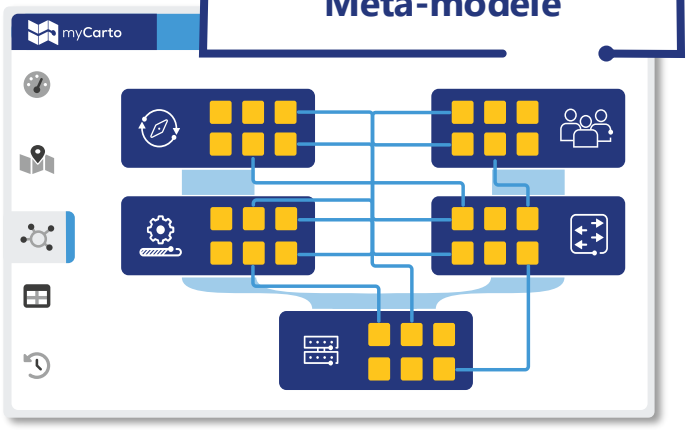
Référentiel

4 fonctionnalités qui font toute la différence

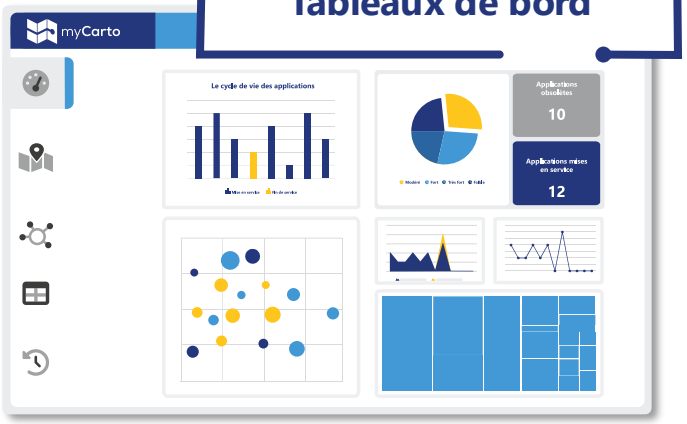
Générateur de cartes



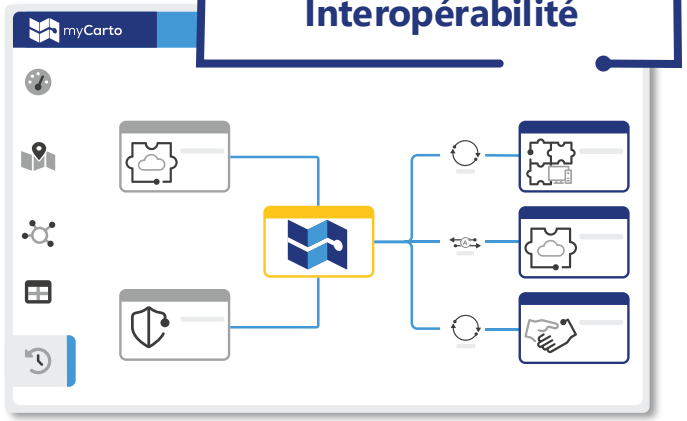
Méta-modèle



Tableaux de bord



Interopérabilité



Offre de service globale

sesan
SERVICE NUMÉRIQUE DE SANTÉ

AB SOFTWARE

Expertise Santé

Expertise SSI

Solution hébergée par le SESAN

Méthodologie projet

Expertise Urbanisation des SI

Expertise Produit

Support, formation et accompagnement

Offre dédiée aux adhérents du SESAN

- Base myCarto et template prêt à l'emploi
- Expertise d'initialisation éprouvée
- Offre packagée Setup / Formation / Licences SAAS
- Hébergement HDS par le SESAN

Pour poursuivre…
Rendez-vous sur le Stand

AB SOFTWARE

Thibaut DEQUENNE
Directeur commercial

Cédric VOLANDI
Directeur Général

TOUS CYBER VIGILANTS

sesan
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Pause déjeuner et visite des stands