RGPD : cas pratiques

Café CPTS#14 – octobre 2023

1 Rappel des éléments du RGPD

RGPD : rappel

- ✓ Encadre la mise en œuvre des **traitements des données à caractère personnel**.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

- ✓ Fixe les conditions dans lesquelles de telles données peuvent être légalement collectées, conservées et exploitées par les organismes publics et privés (entreprises, administrations, collectivités, associations…).

- ✓ Vise à éviter que l'utilisation des informations en cause portent atteinte aux droits et libertés des personnes qu'elles concernent.

- *Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles*
- *Le Règlement Général sur la Protection des Données : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*

Qu’est-ce qu’une donnée personnelle ?

IDENTIFICATION

DIRECTEMENT
nom, prénom, photo…

INDIRECTEMENT
numéro de téléphone
plaque d’immatriculation,
numéro de sécurité sociale
adresse postale ou courriel
la voix
l’image

A PARTIR
D’UNE SEULE DONNÉE *(nom)*
ou
DU CROISEMENT D’UN ENSEMBLE DE DONNÉES
(une femme vivant à telle adresse, née tel jour et membre dans telle association)

Et une donnée sensible ?

Numéro d'inscription au répertoire
(NIR, numéro de sécurité sociale)

Données
génétiques et biométriques

Infractions
condamnations pénales
mesures de sûreté

Orientation sexuelle
Vie sexuelle

Appartenance à un syndicat

Données de santé
(santé physique ou mentale)

Opinions
politique, philosophique
Convictions religieuses

Origine
raciale ou ethnique

Collecte des données sensibles

Possible uniquement sous certaines conditions :

Consentement de la personne (actif, explicite, libre, éclairé, spécifique et univoque)

Données concernant les **membres ou les adhérents d'un organisme à but non lucratif** (politique, religieux, philosophique ou syndical)

Données nécessaires à la sauvegarde de la vie humaine

Données rendues publiques par la personne concernée

Justification par l'intérêt public et autorisée par la CNIL

Collecte des données sensibles

Possible uniquement sous certaines conditions :

Consentement de la personne (actif, explicite, libre, éclairé, spécifique et univoque)

Justification par l'intérêt public et autorisée par la CNIL

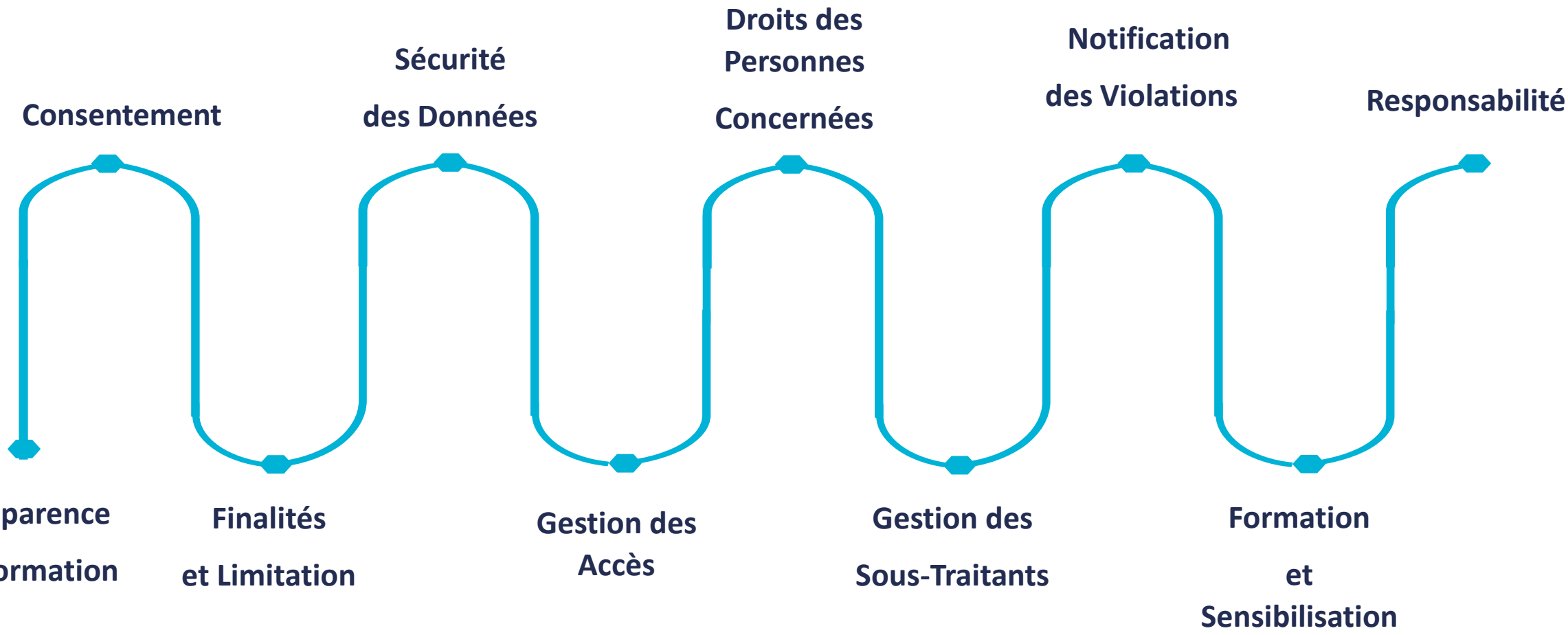
Données concernant les **membres ou les adhérents d'un organisme à but non lucratif** (politique, religieux, philosophique ou syndical)

Données rendues publiques par la personne concernée

Données nécessaires à la sauvegarde de la vie humaine

2 Les obligations des CPTS

Les attendus



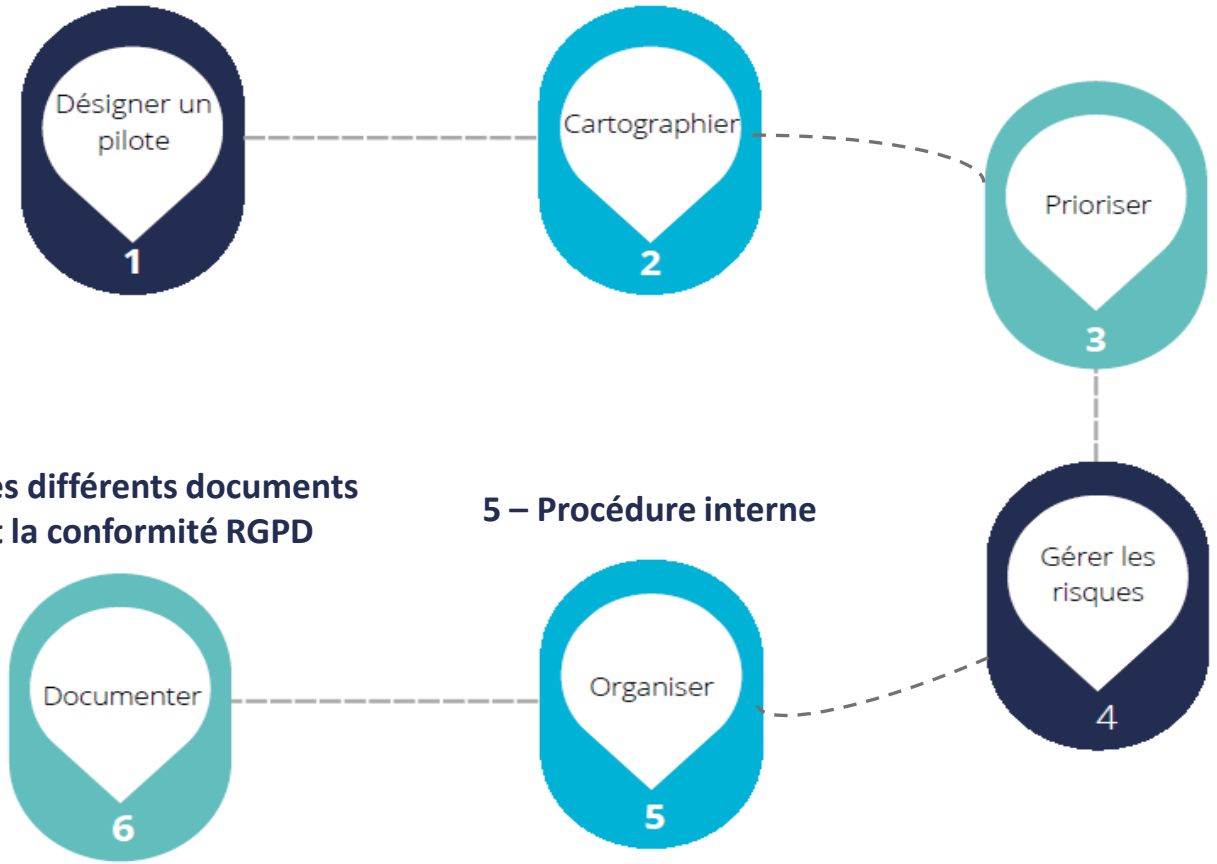
Il s’agit d’obligations de moyens et non d’une obligation de résultats

Etapes du processus RGPD

1- Pilote +/- DPO

2- : Qui ? Quoi ? Pourquoi ? Où ? Jusqu'à quand ? Comment ?

3- Questionnement sur les risques : Pertinence et nécessité de la collecte, choix de la base juridique, information aux personnes de la collecte de données et sa finalité



4- Lister les risques + analyse d'impact si données sensibles traitées

5 – Procédure interne

6- Fournir les différents documents prouvant la conformité RGPD

Responsable de traitement (RT) - Data Protection Officer (DPO)

RT = personne, autorité publique, société ou organisme **qui détermine les finalités et les moyens de ce fichier**, qui décide de sa création.

→ *Ici la CPTS, incarnée par son représentant légal (président).*

En cas de non-conformité de l'organisme au RGPD, c'est le principe de co-responsabilité du responsable au traitement (donc l'organisme) et des sous-traitants qui s'applique.

DPO = personne ayant pour fonction principale **d'assurer la mise en conformité de l'organisme au RGPD**. **Le DPO n'est pas obligatoire en CPTS sauf en cas de données sensibles traitées.**

- Cartographier les traitements de données effectués par l'organisme
- Participer à l'établissement des règles internes en matière de RGPD
- Recenser l'ensemble des activités de traitement mises en œuvre par l'organisme

→ *Ne dispose pas de pouvoir décisionnel concernant la finalité et les moyens du traitement des données personnelles.*

→ *En cas de non-conformité, la responsabilité du DPO ne peut pas être engagée.*

Le DPO doit posséder des connaissances spécialisées en matière de protection des données.

Le DPO ne doit pas être entravé dans sa mission.

3 Cas pratiques en CPTS

Principales données traitées en CPTS

Données concernant les salariés
de la CPTS

Données concernant les adhérents à la CPTS (noms, prénoms, adresses, e-mails récoltés via les bulletins d'adhésion, annuaire, envoi de newsletters, organisation d'événements et de formations...)

+/- Données de santé récoltées dans le cadre de ses missions comme par exemple des actions de coordination du parcours de soins et même de mise en lien patients-médecins traitants / Ou des données de santé des salariés

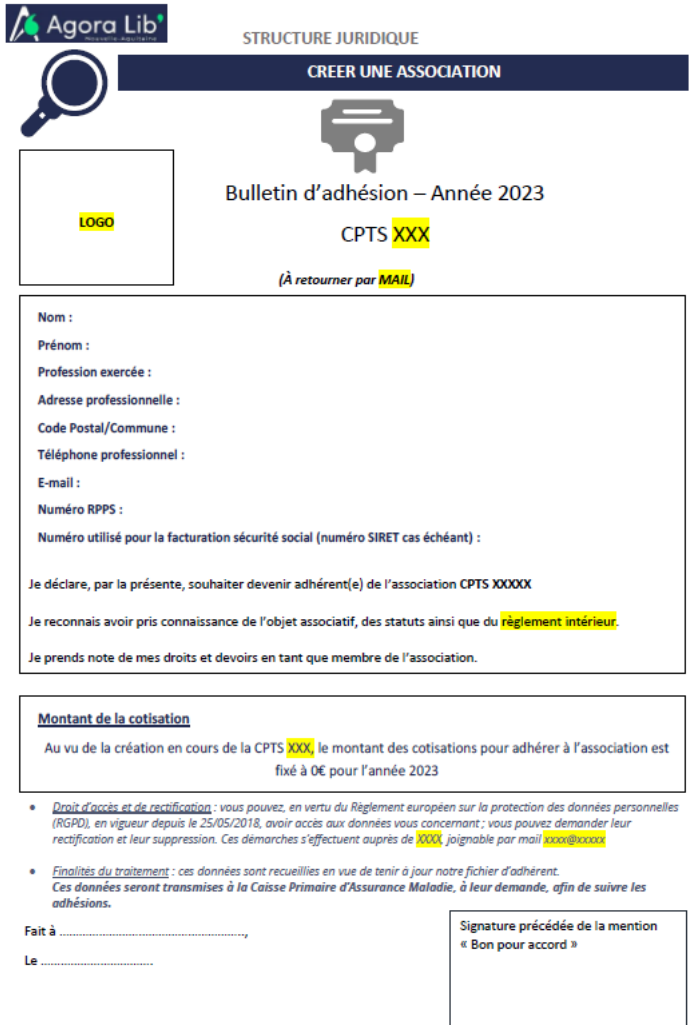
A faire / A ne pas faire

- Formaliser une procédure de traitement de données conforme dès le départ
- Sécuriser les données
- Se faire accompagner : en interne si les ressources sont disponibles ou en externe par des personnes spécialisées.

- Communiquer des données sensibles par des canaux non sécurisés ou partager des identifiants de connexion entre plusieurs membres de la CPTS
- Collecter et conserver des données non utilisées

1) Dans le cas de traitement de données personnelles

Cas 1 – Gestion des adhérents à l'association



Agora Lib

STRUCTURE JURIDIQUE

CREER UNE ASSOCIATION

LOGO

Bulletin d'adhésion – Année 2023

CPTS XXX

(À retourner par MAIL)

Nom :

Prénom :

Profession exercée :

Adresse professionnelle :

Code Postal/Commune :

Téléphone professionnel :

E-mail :

Numéro RPPS :

Numéro utilisé pour la facturation sécurité social (numéro SIRET cas échéant) :

Je déclare, par la présente, souhaiter devenir adhérent(e) de l'association **CPTS XXXXX**

Je reconnais avoir pris connaissance de l'objet associatif, des statuts ainsi que du règlement intérieur.

Je prends note de mes droits et devoirs en tant que membre de l'association.

Montant de la cotisation

Au vu de la création en cours de la CPTS XXX, le montant des cotisations pour adhérer à l'association est fixé à 0€ pour l'année 2023

- *Droit d'accès et de rectification : vous pouvez, en vertu du Règlement européen sur la protection des données personnelles (RGPD), en vigueur depuis le 25/05/2018, avoir accès aux données vous concernant ; vous pouvez demander leur rectification et leur suppression. Ces démarches s'effectuent auprès de XXXX, joignable par mail xxxx@xxxxx*
- *Finalités du traitement : ces données sont recueillies en vue de tenir à jour notre fichier d'adhérent.*
  Ces données seront transmises à la Caisse Primaire d'Assurance Maladie, à leur demande, afin de suivre les adhésions.

Fait à .....,

Le .....

Signature précédée de la mention « Bon pour accord »

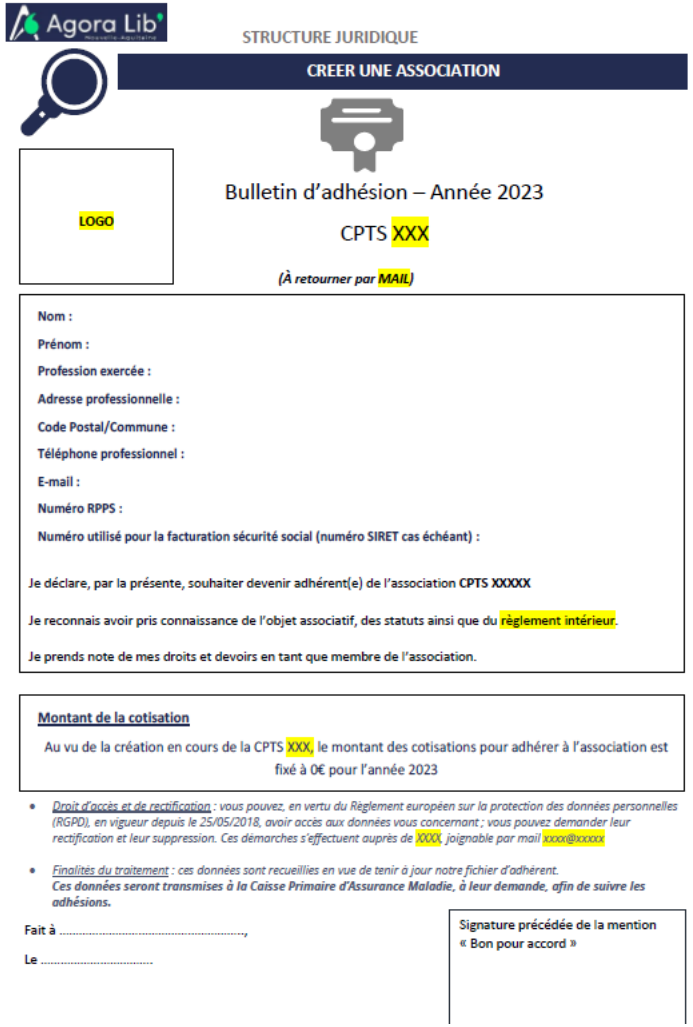
Une CPTS se crée sur le territoire X. Elle a lancé ses adhésions.

De plus, elle indemnise les référents des groupes de travail et les membres du bureau sous forme d'ICPA : pour cela elle tient un registre pour comptabiliser les heures réalisées par chacun et le montant mensuel des indemnisations à verser.

- Gestion de la liste des adhérents à l'association (nom, prénom, numéro adéli, adresse, numéro….)
- Gestion du versement des indemnités compensatrices de perte d'activité (nom, prénom, numéro adéli, RIB…)

1) Dans le cas de traitement de données personnelles

Cas 1 – Gestion des adhérents à l'association



Agora Lib

STRUCTURE JURIDIQUE

CREER UNE ASSOCIATION

LOGO

Bulletin d'adhésion – Année 2023

CPTS XXX

(À retourner par MAIL)

Nom :

Prénom :

Profession exercée :

Adresse professionnelle :

Code Postal/Commune :

Téléphone professionnel :

E-mail :

Numéro RPPS :

Numéro utilisé pour la facturation sécurité social (numéro SIRET cas échéant) :

Je déclare, par la présente, souhaiter devenir adhérent(e) de l'association CPTS XXXXX

Je reconnais avoir pris connaissance de l'objet associatif, des statuts ainsi que du règlement intérieur.

Je prends note de mes droits et devoirs en tant que membre de l'association.

Montant de la cotisation

Au vu de la création en cours de la CPTS XXX, le montant des cotisations pour adhérer à l'association est fixé à 0€ pour l'année 2023

- *Droit d'accès et de rectification : vous pouvez, en vertu du Règlement européen sur la protection des données personnelles (RGPD), en vigueur depuis le 25/05/2018, avoir accès aux données vous concernant ; vous pouvez demander leur rectification et leur suppression. Ces démarches s'effectuent auprès de XXXX, joignable par mail xxxx@xxxxx*
- *Finalités du traitement : ces données sont recueillies en vue de tenir à jour notre fichier d'adhérent.*
  Ces données seront transmises à la Caisse Primaire d'Assurance Maladie, à leur demande, afin de suivre les adhésions.

Fait à .....,

Le .....

Signature précédée de la mention « Bon pour accord »

Problématiques posées par l'action :

- Traitement de données personnelles (Nom, prénom, numéro adéli, RIB….)

Bonnes pratiques et solutions :

1) Registre de traitement à remplir
2) Enregistrement dans un fichier sécurisé ou espace de stockage sécurisé
3) Information des adhérents sur l'utilisation des données (mentions sur le bulletin d'adhésion) : finalités du traitement

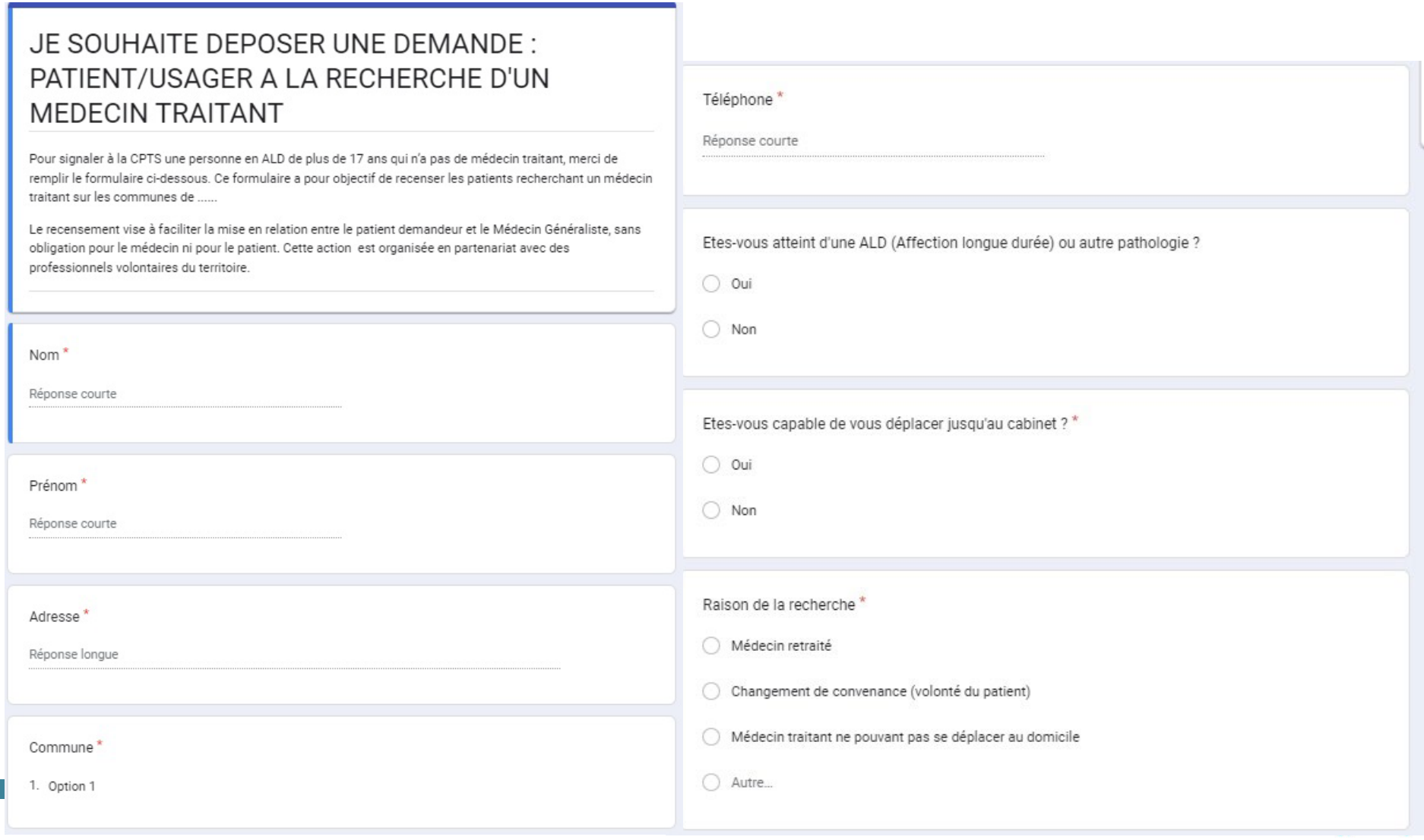
2) Dans le cas de traitement de données sensibles

Cas 2 - Mise en lien patients - médecin traitant via un questionnaire

Une CPTS met en place une action permettant de mettre en lien les patients cherchant un médecin traitant et les médecins du secteur.

Pour cela, elle met en place un formulaire de demande, destiné aux usagers et aux PS.

Mais certaines informations récoltées (« êtes-vous atteint d'une ALD?) font partie de la liste des données sensibles (données de santé).



JE SOUHAITE DEPOSER UNE DEMANDE : PATIENT/USAGER A LA RECHERCHE D'UN MEDECIN TRAITANT

Pour signaler à la CPTS une personne en ALD de plus de 17 ans qui n'a pas de médecin traitant, merci de remplir le formulaire ci-dessous. Ce formulaire a pour objectif de recenser les patients recherchant un médecin traitant sur les communes de .....

Le recensement vise à faciliter la mise en relation entre le patient demandeur et le Médecin Généraliste, sans obligation pour le médecin ni pour le patient. Cette action est organisée en partenariat avec des professionnels volontaires du territoire.

Nom *
Réponse courte

Prénom *
Réponse courte

Adresse *
Réponse longue

Commune *
1. Option 1

Téléphone *
Réponse courte

Etes-vous atteint d'une ALD (Affection longue durée) ou autre pathologie ?
- Oui
- Non

Etes-vous capable de vous déplacer jusqu'au cabinet ? *
- Oui
- Non

Raison de la recherche *
- Médecin retraité
- Changement de convenance (volonté du patient)
- Médecin traitant ne pouvant pas se déplacer au domicile
- Autre...

2) Dans le cas de traitement de données sensibles

Cas 2 - Mise en lien patients - médecin traitant via un questionnaire

JE SOUHAITE DEPOSER UNE DEMANDE : PATIENT/USAGER A LA RECHERCHE D'UN MEDECIN TRAITANT

Pour signaler à la CPTS une personne en ALD de plus de 17 ans qui n'a pas de médecin traitant, merci de remplir le formulaire ci-dessous. Ce formulaire a pour objectif de recenser les patients recherchant un médecin traitant sur les communes de .....

Le recensement vise à faciliter la mise en relation entre le patient demandeur et le Médecin Généraliste, sans obligation pour le médecin ni pour le patient. Cette action est organisée en partenariat avec des professionnels volontaires du territoire.

Nom *

Réponse courte

Prénom *

Réponse courte

Adresse *

Réponse longue

Commune *

1. Option 1

Problématiques posées par l'action :

- Traitement de données dites sensibles à la question des ALD

Bonnes pratiques et solutions :

1) Registre de traitement à remplir
2) Enlever les questions qui relèvent de la donnée sensible
3) Procédure interne claire
4) Choix d'outils en conséquence : questionnaire sur une plateforme sécurisée (au moins européen), utilisation d'une messagerie sécurisée et/ou accès à une plateforme d'échanges sécurisée pour échanger avec les médecins
5) Informer les patients des finalités du traitement

2) Dans le cas de traitement de données sensibles

Cas 2 - Mise en lien patients - médecin traitant via un questionnaire

JE SOUHAITE DEPOSER UNE DEMANDE : PATIENT/USAGER A LA RECHERCHE D'UN MEDECIN TRAITANT

Pour signaler à la CPTS une personne en ALD de plus de 17 ans qui n'a pas de médecin traitant, merci de remplir le formulaire ci-dessous. Ce formulaire a pour objectif de recenser les patients recherchant un médecin traitant sur les communes de .....

Le recensement vise à faciliter la mise en relation entre le patient demandeur et le Médecin Généraliste, sans obligation pour le médecin ni pour le patient. Cette action est organisée en partenariat avec des professionnels volontaires du territoire.

Nom *

Réponse courte

Prénom *

Réponse courte

Adresse *

Réponse longue

Commune *

1. Option 1

Problématiques posées par l'action :
- Traitement de données dites sensibles à la question des ALD

SINON
1) DPO Obligatoire
2) Analyse des risques à réaliser par le responsable de traitement, avec l'aide du DPO
3) Procédure interne claire : *Destruction des données une fois le patient mis en lien ou Anonymisation des données après traitement*
4) Choix d'outils en conséquence : Hébergeur de données de santé agréé ou certifié

2) Dans le cas de traitement de données sensibles

Cas 3 - Mise en place d'un parcours

	A	B	C	D	E	F	G
1	Nom du patient	Prénom du patient	Nom du PS de la PEC	Prénom du PS de la PEC	Profession du PS	Date du début de parcours	Date de fin de parcours
2							
3							
4							
5							
6							

Une CPTS met en place un parcours centré sur l'accompagnement des personnes diabétiques.

Pour suivre ses indicateurs, elle recense dans un fichier Excel les patients ayant bénéficié du parcours.

Mais ces informations font partie de la liste des données sensibles (données de santé).

De plus, comment est transmise et collectée la donnée ?

2) Dans le cas de traitement de données sensibles

Cas 3 - Mise en place d'un parcours diabétologie

	A	B	C	D	E	F	G
1	Nom du patient	Prénom du patient	Nom du PS de la PEC	Prénom du PS de la PEC	Profession du PS	Date du début de parcours	Date de fin de parcours
2							
3							
4							
5							
6							

Problématiques posées par l'action :

- Traitement de données dites sensibles si on fait le lien entre l'identité du patient et la pathologie (donnée de santé)

Bonnes pratiques et solutions :

1) Registre de traitement à remplir
2) Ne pas faire de lien entre la pathologie et les noms des patients
3) Stocker le fichier de manière sécurisée
4) Informer les patients des finalités du traitement

2) Dans le cas de traitement de données sensibles

Cas 3 - Mise en place d'un parcours diabétologie

	A	B	C	D	E	F	G
1	Nom du patient	Prénom du patient	Nom du PS de la PEC	Prénom du PS de la PEC	Profession du PS	Date du début de parcours	Date de fin de parcours
2							
3							
4							
5							
6							

Problématiques posées par l'action :
- Traitement de données dites sensibles si on fait le lien entre l'identité du patient et la pathologie (donnée de santé)

SINON
1) DPO Obligatoire
2) Analyse des risques à réaliser par le responsable de traitement, avec l'aide du DPO
3) Procédure interne claire
4) Choix d'outils en conséquence : Hébergeur de données de santé agréé ou certifié, utilisation des messageries sécurisées et/ou accès à une plateforme d'échange sécurisée pour échanger entre professionnels

2) Dans le cas de traitement de données sensibles

Cas 4 - Mise en place de réunions de concertation pluriprofessionnelle (RCP)

Une CPTS met en place des réunions de concertation pluriprofessionnelle.

La CPTS reçoit les dossiers des patients en amont des réunions.

Or, certains croisements d'informations peuvent rendre les données identifiables.

De plus, la CPTS ne possède pas de messagerie sécurisée ou de plateforme sécurisée.

2) Dans le cas de traitement de données sensibles

Cas 4 - Mise en place de réunions RCP

Problématiques posées par l'action :
- Traitement de données dites sensibles si on fait le lien entre l'identité du patient et la pathologie (donnée de santé)
- Transmission et la collecte des dossiers patients à la CPTS

Bonnes pratiques et solutions :
1) Registre de traitement à remplir
2) Diffusion des bonnes pratiques aux adhérents concernant le partage des dossiers + consentement du patient au préalable
3) La CPTS reste uniquement sur une partie organisationnelle pour ce type de réunions

2) Dans le cas de traitement de données sensibles

Cas 4 - Mise en place de réunions RCP

Problématiques posées par l'action :
- Traitement de données dites sensibles si on fait le lien entre l'identité du patient et la pathologie (donnée de santé)
- Transmission et la collecte des dossiers patients à la CPTS

SINON
1) DPO Obligatoire
2) Analyse des risques à réaliser par le responsable de traitement, avec l'aide du DPO
3) Procédure interne claire
4) Choix d'outils en conséquence : Hébergeur de données de santé agréé ou certifié, utilisation des messageries sécurisées et/ou accès à une plateforme d'échange sécurisée pour échanger entre professionnels

En cas de violation de données

En notifier la CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS dans un délai de 72h

https://notifications.cnil.fr/notifications/index

N’oubliez pas :
Il s’agit d’obligations de moyens et non d’une obligation de résultats

4 Outils nécessaires aux CPTS

Les outils d'aide à la procédure RGPD

Outils internes à la CPTS

Procédure interne

Analyse d'impact (en cas traitement de données sensibles)

Registre des traitements

Formulaires de recueil du consentement, mentions d'informations utilisées

Politiques de gestion des droits des personnes, de conservation des données, de confidentialité

Charte informatique

Plan et registre des violations de données

Outils de sécurisation des données échangées

Messagerie sécurisée

Elaboration de questionnaire
https://framaforms.org/abc/fr/

Hébergeurs de santé :
https://esante.gouv.fr/offres-services/hds/liste-des-herbergeurs-certifies

Drive sécurisé : proton drive
https://proton.me/fr/drive

Conteneur sécurisé :
https://www.primx.eu/fr/zed-free/

Formation et externalisation DPO

Formation DPO

- Nombre d'heures : 35h
- Coût formation : 1500-3000 euros

Externalisation

- Coût : dépendant de la taille de la CPTS et des attendus (mise en conformité et/ou DPO)
- Possibilité de mutualiser entre différentes CPTS

Pour aller plus loin…
MOOC RGPD

Mutualisation d'un DPO au niveau régional ?

En cas de questions supplémentaires :

secretariat@agoralib.org

cybersecurite@esea-na.fr

ESEA e-santé en action NOUVELLE-AQUITAINE

Agora Lib' Nouvelle-Aquitaine