DÉFINITIONS

A noter : toutes les informations sont issues de la CNIL : www.cnil.fr/fr

Le registre des traitements de données : permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que vous faites avec les données personnelles. Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité.

Texte de loi : www.cnil.fr/fr/cnil-direct/question/professionnels-de-sante-avec-le-rgpd-faut-il-encore-declarer-vos-fichiers-la

Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Sa désignation est **obligatoire dans certains cas**. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions. Pour garantir l'effectivité de ses missions, le délégué doit disposer de qualités professionnelles et de connaissances spécifiques et doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement adéquats.

En pratique : vous, le médecin désigné, le pharmacien responsable de l'officine, etc.

Un traitement est toute **opération portant sur des données personnelles**, quel que soit le procédé utilisé. Par exemple, enregistrer, organiser, conserver, modifier, rapprocher avec d'autres données, transmettre, etc. des données personnelles.

Un traitement n'est donc pas uniquement un fichier, une base de données ou un tableau Excel.

Il peut s'agir aussi d'une installation de vidéosurveillance, d'un système de paiement par carte bancaire ou de reconnaissance biométrique, d'une application pour smartphone, etc. ;
Des traitements apparaissent et évoluent selon les innovations technologiques.

Un traitement de données à caractère personnel peut être informatisé ou non.

Un fichier papier organisé selon un plan de classement, des formulaires papiers nominatifs ou des dossiers de candidatures classés par ordre alphabétique ou chronologique sont aussi des traitements de données personnelles.

Le responsable de traitement :

Le responsable d'un traitement de données à caractère personnel est en principe la personne, l'autorité publique, la société ou l'organisme qui **détermine les finalités et les moyens de ce fichier**, qui décide de sa création.

En pratique, il s'agit généralement de la **personne morale** (entreprise, collectivité, etc.) incarnée par son représentant légal (président, maire, etc.).

C'est lui qui **doit accomplir**, lorsque cela est encore obligatoire comme, par exemple, dans le domaine de la santé, les **formalités déclaratives auprès de la CNIL**.

En pratique : souvent le DPO pour les petites structures.

Une donnée « sensible » est une information qui révèle la prétendue **origine raciale** ou **ethnique,** les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance **syndicale**, ainsi que le **traitement des données génétiques**, des **données biométriques** aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données relatives à la **vie sexuelle** ou à l'**orientation sexuelle** d'une personne physique. Le RGPD interdit de recueillir ou d'utiliser ces données, sauf dans certains cas :

- si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique et informée) ;
- si les informations sont rendues publiques par la personne concernée ;
- si elles sont nécessaires à la sauvegarde de la vie humaine ;
- si leur utilisation est justifiée par l'intérêt public et autorisée par la CNIL ;
- si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

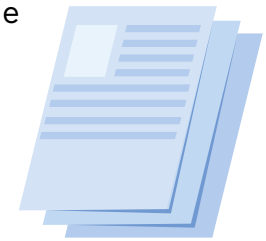
Une donnée personnelle est toute information se rapportant à une **personne physique identifiée ou identifiable**. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise.

Une personne physique peut être identifiée :

- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- à partir d'une seule donnée (exemple : nom) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association).



Par contre, des coordonnées d'entreprises (par exemple, l'entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie1[@]email.fr ») ne sont pas, en principe, des données personnelles.

Liens utiles : CNIL et cabinets médicaux :

Cabinets médicaux et paramédicaux à titre libéral : que faire ?

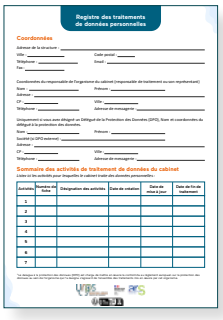
La CNIL publie trois référentiels pour le secteur de la santé

MÉTHODE

Qui met en place le registre ?

Quelle que soit la taille de votre structure, vous devez identifier un « délégué à la protection des données » (DPO) pour mettre en place et être responsable de ce registre. Dans les petites structures, cela peut-être VOUS, ou un de vos salariés ; pas besoin d'avoir recours à un prestataire extérieur.

Comment faire ?

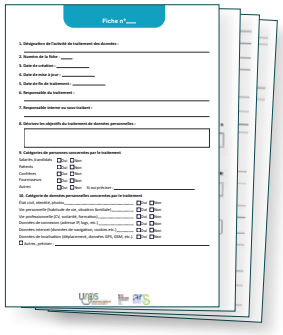


1. Remplir la page de garde

Le document « page de garde vierge » est à télécharger ici

2. Remplir la ou les fiches de traitement

Le document « fiche de traitement vierge » est à télécharger ici autant de fois que vous avez de base de données dans votre structure.



Une base de données = une fiche de traitement

Vous avez fini, bravo ! 😊

Et après ?

Ce registre doit être actualisé.

Nous vous conseillons de le faire une fois par an et lorsque :

- La personne en charge du registre change
- Une base de données est modifié (exemple : ajout/ suppression d'un critère)
- Vous créer une nouvelle base de données (salariés, fournisseurs, etc.)

Pour vos collègues et collaborateurs

Le registre doit pouvoir être consulté par tout collaborateur du cabinet ayant vocation à mettre en œuvre des traitements de données. Il est donc essentiel de sensibiliser et de former les collaborateurs. Il est conseillé d'intégrer les principes de sécurisation des données personnelles dans le règlement intérieur s'il existe.

Pour ce faire, n'hésitez pas à leur faire consulter le replay du webinaire RGPD : https://youtu.be/ktPAk6iVLZo?si=G_LNGcp8N35BxNSu

URPS Médecins Libéraux Hauts-de-France – Nord-Pas de Calais / Picardie

République Française – Liberté, Égalité, Fraternité

ARS Agence Régionale de Santé Hauts-de-France

Le tri facile

Registre des traitements de données personnelles

Coordonnées

Adresse : 1 rue des cerisiers

Ville : LILLE

Code postal : 59000

Téléphone : 03.21.03.21.03

Email : dr.jacquescaron@test.fr

Fax : /

Coordonnées du responsable de l'organisme du cabinet (responsable de traitement ou son représentant)

Nom : CARON

Prénom : Jacques

Adresse : 1 rue des cerisiers

CP : 59000

Ville : LILLE

Téléphone : 06.01.02.03.04

Adresse de messagerie : jacquescaron59@test.fr

Uniquement si vous avez désigné un Délégué de la Protection des Données (DPO)[1], Nom et coordonnées du délégué à la protection des données.

Nom :

Prénom :

Société (si DPO externe) :

Adresse :

CP :

Ville :

Téléphone :

Adresse de messagerie :

Sommaire des activités de traitement de données du cabinet

Listez ici les activités pour lesquelles le cabinet traite des données personnelles :

Activités	Numéro de fiche	Désignation des activités	Date de création	Date de mise à jour	Date de fin de traitement
1	F-1	Création d'un dossier patient	06/06/2024	06/06/2024	
2					
3					
4					
5					
6					
7					

[1] Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Fiche n°1

1. Désignation de l'activité de traitement des données :

Création d'un dossier patient

2. Numéro de la fiche : 1

3. Date de création : 06/06/2024

4. Date de mise à jour : _____

5. Date de fin de traitement : _____

6. Responsable du traitement :

Dr CARON Jacques

7. Responsable interne ou sous-traitant :

Dr CARON Jacques

8. Décrivez les objectifs du traitement de données personnelles :

Constituer le dossier des patients dans le logiciel métier

9. Catégories de personnes concernées par le traitement

Salariés /candidats	☐ Oui	☑ Non	
Patients	☑ Oui	☐ Non	
Confrères	☐ Oui	☑ Non	
Fournisseurs	☐ Oui	☑ Non	
Autres	☐ Oui	☑ Non	Si oui préciser : _____

10. Catégorie de données personnelles concernées par le traitement

État civil, identité, photos	☑ Oui	☐ Non
Vie personnelle (habitude de vie, situation familiale)	☑ Oui	☐ Non
Vie professionnelle (CV, scolarité, formation)	☑ Oui	☐ Non
Données de connexion (adresse IP, logs, etc.)	☐ Oui	☑ Non
Données internet (données de navigation, cookies etc.)	☐ Oui	☑ Non
Données de localisation (déplacement, données GPS, GSM, etc.).	☐ Oui	☑ Non

☐ Autres, préciser : _____

11. Données personnelles sensibles contenues dans le traitement

Donnée relevant de l'origine raciale ou ethnique	☑ Oui	☐ Non
Données révélant d'opinions politiques	☐ Oui	☑ Non
Données révélant de conviction religieuse ou philosophique	☐ Oui	☑ Non
Données concernant la vie ou l'orientation sexuelle	☑ Oui	☐ Non
Données révélant l'appartennances syndicale	☐ Oui	☑ Non
Numéro d'identification national unique (NIR/INS)	☑ Oui	☐ Non
Données concernant la santé	☑ Oui	☐ Non
Données génétiques	☑ Oui	☐ Non
Données biométriques aux fins d'identifier une personne physique de manière unique	☑ Oui	☐ Non
Donnée concernant des mineurs de moins de 16 ans	☑ Oui	☐ Non
Données pénales ou infractions	☐ Oui	☑ Non

12.Rétention des données personnelles

Les données personnelles sont conservées pendant :

☐ Jours ☐ Mois ☐ Années ☑ Durée indéterminé

Si vous ne pouvez pas définir une donnée chiffrée, veuillez préciser les critères utilisés pour déterminer le délai d'effacement des données personnelles.

20 ans à compter de la date de la dernière consultation du patient

13. Rétention des données personnelles sensibles

Les données personnelles sensibles sont conservées pendant

☐ Jours ☐ Mois ☐ Années ☑ Durée indéterminé

Si vous ne pouvez pas définir une donnée chiffrée, veuillez préciser les critères utilisés pour déterminer le délai d'effacement des données personnelles sensibles.

20 ans à compter de la date de la dernière consultation du patient

14. Destinataire des données personnelles

Les données personnelles sont transmises à des destinataire internes au cabinet : ☑ Oui ☐ Non

Si oui préciser le service et le degré de confidentialité

Sont partagées avec le secrétariat et a la possibilité de les mettre à jour

Les données personnelles sont transmises à des destinataire externes au cabinet

Cabinet d'un confrère ☐ Oui ☑ Non

Si oui préciser le nom, adresse, nom du responsable, téléphone, mail, le degré de confidentialité.

Établissement de santé ☐ Oui ☑ Non

Si oui préciser le nom, adresse, nom du responsable, téléphone, mail, le degré de confidentialité.

Établissement médico-sociale ☐ Oui ☑ Non

Si oui préciser le nom, adresse, nom du responsable, téléphone, mail, le degré de confidentialité.

Sous-traitant (exemple : Groupement Employeur, comptable) ☐ Oui ☑ Non

Si oui préciser le nom, adresse, nom du responsable, téléphone, mail, le degré de confidentialité.

Autre :

15. Destinataire des données personnelles sensibles

Les données personnelles sensibles sont transmises à des destinataire internes au cabinet :

☐ Oui ☑ Non

Si oui préciser le service et le degré de confidentialité

Les données personnelles sensibles sont transmises à des destinataire externes au cabinet

Cabinet d'un confrère ☐ Oui ☑ Non

Si oui préciser le nom, adresse, nom du responsable, téléphone, mail, le degré de confidentialité.

Établissement de santé ☐ Oui ☑ Non

Si oui préciser le nom, adresse, nom du responsable, téléphone, mail, le degré de confidentialité.

Établissement médico-sociale ☐ Oui ☑ Non

Si oui préciser le nom, adresse, nom du responsable, téléphone, mail, le degré de confidentialité.

Sous-traitant (exemple : Groupement Employeur, comptable), … ☐ Oui ☑ Non

Si oui préciser le nom, adresse, nom du responsable, téléphone, mail, le degré de confidentialité.

Autre :

16. Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ? ☐ Oui ☑ Non

Si oui, vers quel(s) pays :

17. Mesures de sécurité des accès aux locaux

Les accès aux locaux sont contrôlés ☑ Oui ☐ Non

Les postes de traitement sont inaccessibles aux visiteurs ☑ Oui ☐ Non

Les imprimantes de DP* et les documents sont inaccessibles aux visiteurs ☑ Oui ☐ Non

Les accès aux traitements sont tracés ☑ Oui ☐ Non

Si oui, préciser les données enregistrées

Pointage

Les postes de traitement sont protégés par des antivirus, pare-feu ☑ Oui ☐ Non

Dans le cas où cette partie est sous-traitrée, les sous-traitants sont ils controlés ☐ Oui ☐ Non

☑ Non Communiqué

* DP = Données Personnelles