RGPD – Règlement général de protection des données – 21 mars 2019

Sommaire :

RGPD – Règlement général de protection des données - en application depuis le 25 mai 2018

1. Introduction

Il s'agit surtout de **protéger les données de nos patients** plutôt que les nôtres.

La mise en conformité au RGPD minimale peut être simple si on dispose de certains outils.

Le règlement européen est l'instrument législatif le plus puissant de la législation européenne; il confère un niveau d'harmonisation maximal dans tous les pays européens.

Pourquoi protéger les données à caractère personnel (DCP) ?

- ☞ car elles ont de la valeur pour de nombreux acteurs
- ☞ car les technologies évoluent rapidement

A noter que les risques dépendent du contexte et du type de données.

2. Champ d'application

A. MATERIEL

1. Définition

Il se définit en fonction de 2 critères :

- ➢ Y a-t-il des données à caractère personnel ?
- ➢ Ces DCP sont-elles traitées ?

Si la réponse est OUI à chacune des 2 questions, alors le RGPD s'applique.

DCP = toute information se rapportant à une personne physique identifiée ou identifiable[1].

2. Exemples

données d'identification (nom, prénom, adresse IP,...), données financières (n° compte, salaire,...), données physiques (description,...), habitudes de vie, données psychiques (comportement,...), loisirs et centres d'intérêts, données judiciaires, convictions politiques ou religieuses, données médicales ou biométriques, éducation-formation-situation professionnelle, photos-vidéos,...

3. Exclusion

Le RGPD ne s'applique pas aux personnes décédées ni aux sociétés.

[1] Identifiable par exemple au départ d'un n° de compte bancaire, d'une plaque d'immatriculation,…

4. Catégories particulières de données

a) données sensibles

ce sont celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses,...

b) celles qui portent sur :

- la santé au sens large
- la vie sexuelle
- l'orientation sexuelle d'une personne

Ces données sont également visées par le RGPD. L'UDNF ainsi que chacun des praticiens détiennent ces données. Et dans notre pratique quotidienne, nous traitons ces données liées à la santé è il faudra donc être vigilant par rapport au respect du RGPD.

5. Traitement des données

Il s'agit de toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés (informatiquement ou fiches papier classées selon un critère déterminé) et appliquées à des données ou des ensembles de données à caractère personnel.

Même si on ne détient qu'une seule donnée, on tombe sous l'application du RGPD.

B. TERRITORIAL

1. Principe

Le RGPD s'applique :

- sur le territoire de l'Union Européenne, même si les données concernent des non Européens.
- dès qu'on traite des données de citoyens européens, même si la société est située en dehors de l'Union Européenne.

2. Exceptions

Il en existe cinq, mais une seule est intéressante du point de vue de l'UDNF : le RGPD ne s'applique pas aux traitements effectués dans le cadre d'une activité strictement personnelle ou domestique; exemples : données reprises sur un agenda privé ou partagées sur une page facebook **privée** (mais attention RGPD s'applique si page professionnelle ou blog).

3. Sept Grands Principes

- Licéité (loyauté et transparence)
- Limitation des finalités
- Minimisation des données
- Exactitude
- Limitation de la conservation
- Intégrité et confidentialité
- Responsabilité

1. Principe de licéité

Si on veut traiter des données, il faut une base légale; si on n'en a pas, on ne peut pas le faire. On a le choix entre six raisons qui nous permettent de traiter des DCP :

- consentement (devrait être le dernier recours)
- relation contractuelle
- obligation légale
- intérêt vital
- intérêt public (autorité publique)
- intérêt légitime du responsable du traitement ou du tiers

1.1. Relation contractuelle

Dans le cadre de notre relation thérapeute / patient, nous avons besoin de certaines données. On peut traiter ces données si on a l'obligation contractuelle de le faire, ce qui est précisément le cas dans le cadre d'une relation entre le nutrithérapeute et son patient. Et donc, on n'a pas besoin du consentement.

1.2. Obligation légale

Exemple : contrôle fiscal : le comptable ne doit pas demander le consentement de son client pour donner au fisc des factures où apparaissent ses nom et prénom.

1.3. Intérêt vital

Si un intérêt vital est en jeu, on n'a pas besoin du consentement. Exemple : communication de données entre hôpitaux si notre état est jugé grave.

1.4. Intérêt public

Exemple : une administration communale ne demande pas l'autorisation de donner notre nom et notre prénom si un membre de notre famille demande une composition de ménage.

1.5. Intérêt légitime

Celui qui détient des données doit se demander s'il a un intérêt légitime à effectuer un traitement de ces données. Il faut apprécier cet intérêt légitime par rapport à l'intérêt des personnes. Si l'intérêt légitime prévaut, le traitement des données peut être effectué sans demander le consentement de la personne concernée.

Exemple 1 : une société commerciale a un intérêt légitime à toucher un maximum de personnes (en envoyant mails à grande échelle ou en achetant une base de données). Mais elle doit mettre en balance cet intérêt légitime

avec les intérêts des personnes concernées par ces données (elles ont le droit de ne pas être importunées). Si intérêt légitime > intérêt des personnes è peut effectuer le traitement de données sans demander consentement des personnes concernées.

Exemple 2 : placement de caméras pour surveillance des locaux d'une société. Cette société a un intérêt légitime à assurer la sécurité è ok sans demander le consentement des personnes concernées.

1.6. Consentement : Il est très difficile à mettre en œuvre. Pour être valablement donné, il doit être :

- libre (si c'est mon employeur qui le demande, ce n'est pas libre)
- éclairé (si on nous demande notre consentement mais sans nous préciser ce qu'on va faire de nos données, ce n'est pas éclairé)
- spécifique : il faut un consentement pour chaque traitement de données (envoi de mails, vendre les données, autre traitement,...)
- univoque : il ne doit y avoir aucun doute possible quant au fait qu'il y ait eu consentement.

Problématique des newsletters : auparavant, une pratique répandue consistait à simplement compléter notre adresse mail sur un site et nous étions inscrits à la newsletter. Mais, cette méthode implique la possibilité que l'adresse d'un tiers soit introduite, auquel cas il n'y a pas de consentement de la part de ce tiers. C'est la raison pour laquelle il vaut mieux désormais choisir la méthode double "opt in" lorsqu'il s'agit d'inscription à une newsletter :

- ☞ il y a tout d'abord une inscription sur un site, laquelle génère automatiquement l'envoi d'un mail à destination de la personne qui s'est inscrite
- ☞ c'est en activant un lien obtenu via ce mail reçu que le consentement est donné.

REMARQUE CONCERNANT LES CATEGORIES PARTICULIERES DE DONNEES ET NOTAMMENT CELLES RELATIVES A LA SANTE

Principe : on ne peut pas traiter des données médicales

Exceptions : elles sont au nombre de 10 :

- ➢ si la personne a donné son consentement
- ➢ s'il y a exécution d'obligations en matière de droit du travail ou de sécurité sociale
- ➢ si sauvegarde d'intérêts vitaux
- ➢ gestion des membres (association poursuivant une finalité politique, religieuse,...)
- ➢ données qui ont été rendues publiques
- ➢ constatation, exercice ou défense d'un droit en justice
- ➢ motifs d'intérêt public importants
- ➢ **contexte de soins de santé => dans le cadre de nos consultations, on peut traiter des données médicales**
- ➢ motifs d'intérêt public dans domaine de la santé publique (menaces transfrontalières)
- ➢ archivage dans l'intérêt public (recherche scientifique, historique, statistique)

2. Principe de limitation de finalité

Quand on détient des DCP, on ne peut rien faire qu'on n'ait pas annoncé. Les DCP doivent être collectées pour des finalités déterminées, explicites et légitimes. Pas de finalités secrètes. Ainsi, si notre politique de confidentialité prévoit "traitement de vos DCP pour la gestion de votre dossier", nous ne sommes pas autorisés à échanger ou à vendre les données en question.

3. Principe de minimisation des données

On ne peut détenir des données qui ne nous seraient pas utiles. Si l'on demande un renseignement, c'est en raison du fait que cette donnée doit nous servir.

4. Principe d'exactitude des données

On doit faire en sorte que les données dont on dispose soient toujours correctes. Il ne s'agit pas de téléphoner aux clients/patients toutes les semaines mais bien de mettre en place les moyens nécessaires pour que ces clients/patients puissent corriger leurs données. Si plusieurs services au sein d'une entité -> faire en sorte qu'il y ait une bonne communication.

Il n'y a pas de démarche active à effectuer. Ce qu'il convient de faire, c'est d'intégrer dans nos données les changements que les clients/patients nous communiquent.

5. Principe de limitation de la durée de conservation

Etant donné le fait que les données ne prennent pas de place, il y a tendance à les conserver longtemps. Mais on ne peut les conserver pour une durée qui excède celle qui est strictement nécessaire à ce qu'on en fait. Ex. : si patient a changé de prestataire depuis 20 ans, il faut au moins se poser la question de savoir si l'on a toujours un intérêt à les conserver.

Combien de temps les conserver ?

- Certaines dispositions légales donnent des délais minima (matière fiscale, matière de responsabilité, pour les médecins,...).
- Il faut essayer d'adopter une politique et la respecter. On peut par exemple convenir que le délai de conservation est de 10 ans et essayer de tout faire pour s'y tenir. Cet élément implique notamment qu'on modifie nos outils car, par exemple, les programmes informatiques ne sont pas nécessairement conçus pour qu'on puisse supprimer certaines données.
- Le délai commence à courir à partir du moment où on n'a plus de contact avec la personne concernée.

6. Principe d'intégrité et de confidentialité

C'est le principe le plus important. On doit assurer la sécurité, l'intégrité, la confidentialité sur deux plans

- sur le plan organisationnel : exemple : pas de conservation de données dans la salle d'attente
- sur le plan technique : exemple : au niveau de la gestion informatique, chiffrer ou crypter au moyen d'une clé, un simple mot de passe n'étant pas suffisant.

7. Principe de responsabilité

Signifie qu'on doit pouvoir démontrer qu'on respecte bien les six principes précédents. Si une personne prétend qu'on ne respecte pas le RGPD, elle doit le démontrer : il y a donc renversement de la charge de la preuve.

Il est impératif de documenter notre mise en conformité. Ainsi, par exemple, faut-il tenir une farde ou un fichier où l'on inscrit tout ce que l'on met en place dans ce but. Exemples : tel jour, j'ai communiqué ma politique de confidentialité, j'ai fait mettre une sonnette à ma porte, j'ai soumis mes collaborateurs à une obligation de confidentialité. **Il s'agit de conserver une trace des procédures mises en place**.

4. Droits découlant de l'application de ces principes

Notamment :

1. Transparence et information

Il convient de toujours informer les personnes dont on traite les données sur ce qu'on fait avec leurs données => on a donc l'obligation de communiquer notre politique de confidentialité : que fait-on avec ces données ? quelles données sont demandées ? combien de temps les conserve-t-on ? les transfère-t-on à des tiers ? base légale du traitement ?

Tous ces éléments doivent figurer dans un document clair, synthétique et concis, qui doit être donné au moment où l'on récolte les données, c'est-à-dire quand on adresse le formulaire au client/patient ou quand on enregistre ses données lorsqu'il se présente devant nous.

Outils : distribuer un formulaire ou en cas de newsletter, permettre à la personne de connaître notre politique de confidentialité.

Le plus important des aspects du RGPD, c'est la transparence !

2. Droit d'accès au dossier

Il nous est loisible de nous adresser à toute société et de lui demander si elle traite des données à notre sujet. Délai de réponse : 30 jours. Il y a obligation de répondre à une telle demande même si l'on ne traite aucune donnée.

3. Droit à la rectification et à l'effacement des données

5. Remarque sur la cyber-sécurité

En 2017, deux tiers des entreprises PME ont été victimes de cybercriminalité. Coût : 1 % du P.I.B. Cette criminalité est en hausse.

Lorsqu'on a oublié notre ordinateur ou notre GSM qui ne sont protégés par aucune clé, on a l'obligation d'avertir, dans les 72 heures, les autorités de contrôle ainsi que toutes les personnes dont on dispose des données. A noter que si on ne se dénonce pas => c'est plus grave !

Il convient de prendre conscience que la cybercriminalité est un problème concret et immédiat. On n'a pas besoin d'être ciblé pour être victime d'une attaque.

A noter qu'une empreinte (avec laquelle on peut déverrouiller notre GSM) peut facilement être reproduite avec une imprimante 3D.

Installer un antivirus ne doit pas être la seule mesure à mettre en place; il faut aussi sensibiliser le personnel (exemple : ne pas ouvrir la pièce jointe d'un mail suspect).

6. Obligations qui s'imposent à nous

1. Mise en œuvre de mesures techniques et organisationnelles appropriées et d'une politique adéquate (responsabilité et sécurité)

Caractère **approprié** à la taille de notre structure et au type de données qu'on gère (nom-prénom ou données médicales).

2. Vigilance dans le choix de nos sous-traitants

Vise cas où ce sont des prestataires qui vont traiter des données pour notre propre compte. Exemples : plateforme de stockage de fichiers (onedrive,...), site internet qui contient des adresses mails (c'est notre hébergeur qui stocke nos données).

Si un problème surgit à cause de notre sous-traitant, c'est nous qui en sommes responsables (idem par exemple, qu'un secrétariat social pour un employeur). Si nos données sont stockées en Chine, on ne fait pas preuve de vigilance.

Il y a donc lieu d'interroger nos sous-traitants afin de savoir ce qu'il mettent en place pour la protection des données.

L'obligation pratique qui en découle est d'envisager de conclure un contrat de sous-traitance qui prévoit des clauses prévues par le RGPD (mais évidemment, si on stocke nos données chez Google, c'est inutile car Google a déjà fait le nécessaire sur ce plan).

3. Obligation de notification des violations

Si l'on rencontre un incident du point de vue de la sécurité des données, on a l'obligation de le notifier à tous les clients/patients ainsi qu'à l'autorité de contrôle (exemple : clé USB, GSM ou ordinateur volé ou perdu).

4. Obligation de tenir un registre des activités de traitement

Il se tient au siège social de la société ou de l'association.

Il contient des informations, telles que : toutes les activités de traitement auxquelles on procède, le type de données que l'on détient, la durée de conservation, les mesures prises pour la sécurité.

De manière pratique, généralement, on tient un fichier excel, dont il existe plusieurs modèles sur internet, notamment un modèle conseillé par la CNIL (autorité de protection des données française). Ce document est rempli une fois et tant qu'on n'a pas de nouvelle activité de traitement, on n'y touche pas.

5. Déléguer une personne à la protection des données

Le délégué à la protection des données est chargé de s'assurer que le RGPD est bien respecté au niveau de la structure.

Quand doit-on désigner un délégué à la protection des DCP ?

- si structure de plus de 250 personnes
- si structure :
  - traite des catégories particulières de données (ex.: données médicales)
  - en fait son activité de base (hôpital, cabinet médical, maison de repos)
  - le fait à grande échelle; cette notion n'est pas précisée dans le règlement. Nombre de patients correspondant à 150 ou à 15.000 ? Indice pour cet aspect de "grande échelle" => un cabinet médical avec un médecin : pas de grande échelle, mais si deux médecins, il s'agit bien de grande échelle.

Le délégué à la protection des données peut être une personne interne à la structure pour autant qu'elle n'intervienne pas au niveau décisionnel (donc pas un gérant par exemple).

Il n'y a pas d'exigence de diplômes. Il peut justifier de connaissances spécialisées et approfondies dans le domaine du droit et de la protection des données (soit par des certifications, soit par une expérience probante).

Le poste peut être mutualisé : cinq cabinets médicaux peuvent engager un délégué à la protection des données.

6. Obligation "privacy by default" – "privacy by design"

Lorsque la récolte des données s'effectue vie formulaire, il faut veiller à ce que certaines cases ne soient pas pré-cochées (exemple : "j'accepte que mes données soient diffusées, vendues"). Car si c'est le cas, il y a violation de cette obligation.

7. Réalisation d'une analyse d'impact

Celle-ci doit notamment être envisagée lorsque l'on souhaite développer une nouvelle technologie (par exemple, application qui permette aux patients d'accéder à leur dossier, placement de gps dans les voitures de sociétés,...).

8. Protection lors des transferts de données

Il convient notamment d'être vigilant lors de transferts de données en dehors de l'Union Européenne; il faut vérifier que le prestataire auquel on fait appel offre suffisamment de garanties en matière de protection des données.

7. Sanctions

1. dispensées par l'autorité de contrôle de la protection des données

- ☞ injonctions : tant qu'il n'y a pas de respect du RGPD : plus d'utilisation de données
- ☞ amendes : 4 % du chiffre d'affaires annuel mondial ou 20.000.000 €, le montant le plus élevé étant retenu.

Il est à noter que l'autorité de contrôle a l'obligation de diligenter les plaintes qui lui sont adressées (par un patient mécontent par exemple).

2. sanctions connexes

- perte de contrats et de marchés publics
- perte de partenariats commerciaux
- perte de subsides ou d'agréments
- risque de contentieux importants

8. Mise en conformité

1. désigner un pilote de la MEC, établir une stratégie et une politique de protection des données.

2. sensibiliser, informer et former à la protection des données (notamment pour éviter les erreurs lors de communications téléphoniques).

3. cartographier les traitements et les DCP traitées (!! On détient beaucoup de données médicales) et établir le registre d'activité de traitement.

4. établir rapports d'audits notamment concernant l'aspect légal, informatique, juridique et organisationnel (qui sait avoir accès aux données ?).

5. hiérarchiser les actions à entreprendre (exemple : veiller d'abord à déplacer une armoire avant de régler les aspects liés à l'informatique).

6. organiser les processus internes : une fois le formulaire rentré, où est-il stocké ?

7. documenter la MEC à chaque étape : indiquer au jour le jour les actions entreprises.

En pratique : cinq choses importantes à effectuer

- ☞ Désigner un délégué à la protection des données (note : si trois médecins travaillent ensemble, ce ne peut être aucun des trois ni la secrétaire si elle ne dispose pas de connaissances juridiques de base).
- ☞ Etablir un registre du traitement.
- ☞ Identifier les sous-traitants et revoir les contrats.
- ☞ Adapter les contrats de travail et le règlement de travail. Importance de soumettre nos employés à la confidentialité : prévoir un document qui constituera à la fois l'information et l'obligation de se soumettre à l'obligation de confidentialité. Pas nécessaire si structure médicale au sein de laquelle le secret médical est de mise. Il est à noter que la politique de confidentialité vis-à-vis de nos employés est différente de celle existant à l'égard des patients.
- ☞ Prendre les mesures organisationnelles et techniques évidentes et simples pour remédier aux risques principaux.

L'autorité de protection des données ne va pas, dans un premier temps, exiger une conformité à 100 % (elle aussi, elle est en retard) mais va surtout vérifier que la MEC est entamée.

En pratique, au niveau informatique :

- Envoyer une politique de confidentialité avec le formulaire correspond à la situation idéale. Si c'est trop compliqué à mettre en œuvre, alors il faut essayer de s'en approcher en insérant par exemple un extrait de la politique de confidentialité.

- Si formulaire par internet : placer, de manière bien visible et en évidence, un lien vers la politique de confidentialité. Se référer à ce lien dans le formulaire, c'est donner la possibilité au patient d'en prendre connaissance.

- Si l'on doit obtenir un consentement, il convient d'insérer une case à cocher. Sur un site, il peut être également prévu de cliquer obligatoirement sur un lien avant de pouvoir poursuivre la navigation. Si la personne accepte, cela traduit le fait qu'elle a lu la politique de confidentialité.

- mailings : c'est compliqué !
    - ceux destinés à de potentiels patients : pour savoir si l'envoi de mails non sollicités est autorisé, il faut se référer à la notion d'intérêt légitime (voir supra). En principe, on ne peut envoyer un mail à une personne qui ne s'est jamais adressée à nous.
    - s'il s'agit de documentation => l'intérêt légitime, c'est de l'information; on n'a pas besoin du consentement => la balance est clairement en faveur de la structure => on peut donc envoyer un
    -

Merci chaleureux à **Christine Maissin** pour le travail de transcription et de clarification effectué !

L'équipe de l'UDNF

Editeur Responsable : UDNF – 5 rue Chalais 4530 Fize-Fontaine

EXEMPLE DE REGISTRE

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.

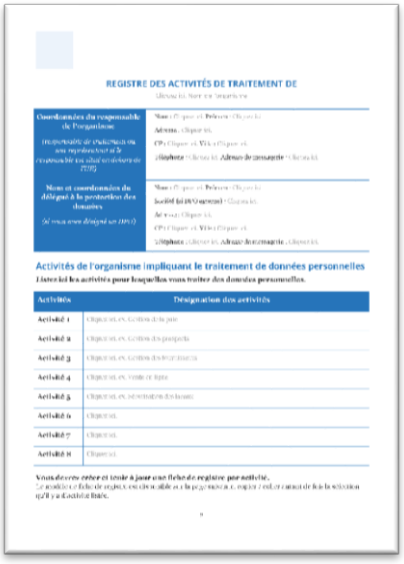
Ce document vise à recenser les traitements de données personnelles mis en œuvre dans votre organisme **en tant que responsable de traitement**. Centralisé et régulièrement mis à jour, il vous permet de répondre à l'obligation de tenir un registre prévue par le RGPD.

Une fois ce recensement effectué, vous serez en mesure de procéder à l'analyse des traitements de données personnelles à la règlementation.

Composition du document

1. La page 2 du registre recense les informations communes à toutes vos activités de traitement.

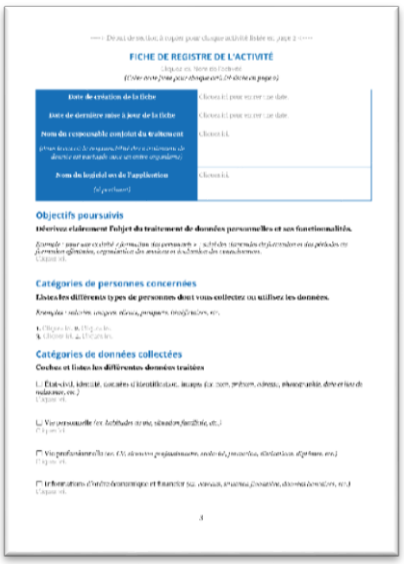
   - Les coordonnées de votre organisme (ou de son représentant sur le territoire européen si votre organisme n'est pas établi dans l'Union européenne).
   - Les coordonnées du délégué à la protection des données (DPO) si vous en disposez.
   - La liste des activités de votre organisme impliquant le traitement de données personnelles.


REGISTRE DES ACTIVITÉS DE TRAITEMENT DE

Activités de l'organisme impliquant le traitement de données personnelles

2. Pour chaque activité recensée, vous devrez créer et tenir à jour une fiche de registre (page 3 à 6).

   Les pages suivantes constituent le modèle de fiche de registre, que vous devrez remplir pour chacune de ces activités.


FICHE DE REGISTRE DE L'ACTIVITÉ

Objectifs poursuivis

Catégories de personnes concernées

Catégories de données collectées

REGISTRE DES ACTIVITÉS DE TRAITEMENT DE

Cliquez ici. Nom de l'organisme

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	Nom : Cliquez ici. Prénom : Cliquez ici. Adresse : Cliquez ici. CP : Cliquez ici. Ville : Cliquez ici. Téléphone : Cliquez ici. Adresse de messagerie : Cliquez ici.
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	Nom : Cliquez ici. Prénom : Cliquez ici. Société (si DPO externe) : Cliquez ici. Adresse : Cliquez ici. CP : Cliquez ici. Ville : Cliquez ici. Téléphone : Cliquez ici. Adresse de messagerie : Cliquez ici.

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités
Activité 1	Cliquez ici. ex. Gestion de la paie
Activité 2	Cliquez ici. ex. Gestion des prospects
Activité 3	Cliquez ici. ex. Gestion des fournisseurs
Activité 4	Cliquez ici. ex. Vente en ligne
Activité 5	Cliquez ici. ex. Sécurisation des locaux
Activité 6	Cliquez ici.
Activité 7	Cliquez ici.
Activité 8	Cliquez ici.

Vous devrez créer et tenir à jour une fiche de registre par activité.
Le modèle de fiche de registre est disponible sur la page suivante, copier / coller autant de fois la sélection qu'il y a d'activité listée.

----> Début de section à copier pour chaque activité listée en page 2 <----

FICHE DE REGISTRE DE L'ACTIVITÉ

Cliquez ici. Nom de l'activité

(Créer cette fiche pour chaque activité listée en page 2)

Date de création de la fiche	Cliquez ici pour entrer une date.
Date de dernière mise à jour de la fiche	Cliquez ici pour entrer une date.
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	Cliquez ici.
Nom du logiciel ou de l'application *(si pertinent)*	Cliquez ici.

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.
Cliquez ici.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Catégories de données collectées

Cochez et listez les différentes données traitées

☐ État-civil, identité, données d'identification, images *(ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*
Cliquez ici.

☐ Vie personnelle *(ex. habitudes de vie, situation familiale, etc.)*
Cliquez ici.

☐ Vie professionnelle *(ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)*
Cliquez ici.

☐ Informations d'ordre économique et financier *(ex. revenus, situation financière, données bancaires, etc.)*
Cliquez ici.

☐ Données de connexion *(ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*
Cliquez ici.

☐ Données de localisation *(ex. déplacements, données GPS, GSM, ...)*
Cliquez ici.

☐ Internet *(ex. cookies, traceurs, données de navigation, mesures d'audience, ...)*
Cliquez ici.

☐ Autres catégories de données *(précisez)* :
Cliquez ici.

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

☐ Oui ☐ Non

Si oui, lesquelles ? :
Cliquez ici.

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

Cliquez ici. Jours, Cliquez ici. Mois, Cliquez ici. Ans, Autre durée : Cliquez ici.

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).
Cliquez ici.

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

(Exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Organismes externes

(Exemples : filiales, partenaires, etc.)

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Sous-traitants

(Exemples : hébergeurs, prestataires et maintenance informatiques, etc.)

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

☐ Oui ☐ Non

Si oui, vers quel(s) pays :
Cliquez ici.

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

Mesures de sécurité

Cochez et décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

☐ Contrôle d'accès des utilisateurs

Décrivez les mesures :

Cliquez ici.

☐ Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs),* les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

Cliquez ici.

☐ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

Cliquez ici.

☐ Sauvegarde des données

Décrivez les modalités :

Cliquez ici.

☐ Chiffrement des données

Décrivez les mesures (*exemple : site accessible en https, utilisation de TLS, etc.)* :

Cliquez ici.

☐ Contrôle des sous-traitants

Décrivez les modalités :

Cliquez ici.

☐ Autres mesures :

Cliquez ici.

----> Fin de section à copier pour chaque activité listée en page 2 <----