MÉMENTO RGPD

SENSIBILISATION AU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

À L'USAGE DU DIRECTEUR D'ÉTABLISSEMENTS

DIRECTION GÉNÉRALE DE L'OFFRE DE SOINS

HOP'EN

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

Le mot de la directrice générale de l'offre de soins

Cécile COURREGES

L'organisation de l'offre de soins doit évoluer en permanence et s'adapter aux besoins du patient et aux nouveaux enjeux de santé publique. Pour renforcer, par exemple l'accès territorial aux soins, il faut pouvoir tirer tout le bénéfice des technologies de l'information et des communications. Le numérique favorise en effet l'échange, le partage, et donc le décloisonnement entre les différents acteurs (offreurs de soins et usagers).

Il favorise la prise en charge ambulatoire en contribuant à des organisations plus efficientes et réduit les distances en permettant de développer la télémédecine. Il porte également, du fait de la masse de données automatisées stockées, un immense potentiel d'information.

Tous ces nouveaux outils, ces nouvelles organisations, ne peuvent se déployer au quotidien que si les patients et les professionnels de santé leur accordent une pleine confiance.

Or, dans un environnement où la numérisation s'accélère et devient omniprésente, de nouveaux risques apparaissent. Il est donc essentiel d'être en situation de pouvoir les comprendre, les évaluer afin de mieux les maîtriser. Les méthodes et outils de la sécurité numérique ne manquent pas, mais ils perdent toute efficacité s'ils ne sont pas soutenus en permanence. Les promouvoir et accompagner leur mise en œuvre relève de la responsabilité des établissements de santé et notamment de celle de leurs managers.

Avec l'entrée en application, le 25 mai 2018, du Règlement Général sur la Protection des Données (RGPD) et la promulgation le 20 juin 2018 de la loi relative à la protection des données personnelles, un nouveau cadre juridique est posé. Il vise à rendre au citoyen le contrôle de ses données personnelles et renforce la responsabilité des organismes qui les gèrent en leur demandant d'assurer une protection optimale à chaque instant.

Le présent mémento a pour objectif d'éclairer les décideurs sur les conséquences, pour les établissements de santé, de ce nouveau contexte règlementaire et d'en préciser les enjeux. Un mémo-quizz « RGPD » disponible à la fin du document propose des repères afin de faciliter la mise en œuvre de la conformité.

Bonne Lecture,

Cécile Courrèges

Les objectifs de ce guide

Face à l'évolution rapide des technologies et à l'utilisation croissante des données personnelles, l'Union européenne a défini de nouvelles dispositions portées par le RGPD afin de :

- Rendre aux citoyens le contrôle de leurs données personnelles
- Créer un niveau élevé et uniforme de protection des données à travers l'Union européenne
- Définir un cadre juridique adapté à l'ère numérique

Le RGPD est un règlement s'appliquant dans tous les pays de l'Union européenne le 25 mai 2018. Il marque le passage d'une logique de formalités préalables à une logique de responsabilisation des acteurs (i.e. démontrer la conformité au travers d'une documentation interne).

Ce guide a pour objectif de vous sensibiliser et de mettre en exergue l'impact du RGPD sur vos établissements au regard de la particularité des données que vous gérez. Il est un complément au guide Cybersécurité publié en 2017 par la DGOS.

Table des matières

Qu'est-ce qu'une donnée à caractère personnel ?

Le RGPD définit comme une donnée à caractère personnel toute information relative à une personne physique identifiée ou pouvant être identifiée, directement ou indirectement.

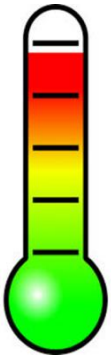
- **Les données à caractère personnel sont des données qui permettent d'identifier directement une personne** (le nom, le prénom, une photo, une vidéo, une adresse mail nominative), **des données indirectement identifiantes** (numéro de sécurité sociale, numéro d'employé, identifiant national de compte bancaire, données biométriques, empreinte digitale, image de la rétine, réseau veineux de la main…) **ou un recoupement d'informations** (le fils du notaire hospitalisé dans notre établissement habitant au 11, bd Raspail à Paris).
- **La définition de donnée à caractère personnel ne vise que les personnes physiques**, elle ne s'applique pas aux personnes morales.

Le terme « DCP » signifie « données à caractère personnel » et sera utilisé dans ce guide pour faire référence à ce que l'on nomme plus communément les « données personnelles ».

Exemple : consultantexterne@etablissement.fr n'est pas une donnée à caractère personnel car c'est une adresse mail non nominative, ne rentrant pas dans le champ du RGPD, pour autant que cette adresse fonctionnelle ne puisse être associée à une seule personne ; dans le cas contraire, elle deviendrait alors indirectement nominative.

Qu'est-ce qu'une donnée à caractère personnel ?

Les données de santé font partie des données à caractère personnel dites « sensibles » au sens du RGPD.



DCP sensibles

Données de santé, données génétiques ou biométriques, opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle ou orientation, origine raciale ou ethnique,

DCP présentant une sensibilité particulière

Numéro de sécurité sociale

DCP courantes

Etat civil (date de naissance, adresse…), données de connexion (adresse IP, journaux, cookies), données de localisation

Vos établissements traitent des données de santé mais pas seulement : le RGPD s'applique également à toutes les DCP que vous traitez, notamment, celles concernant vos employés.

Les données à caractère personnel gérées dans vos établissements

Les données de santé nécessaires à la prise en charge des patients : dossier médical du patient, examens médicaux, etc..;	**Les données de santé ou données à caractère personnel collectées** dans un souci d'amélioration de la prise en charge ou de recherche;	**Les données à caractère personnel non médicales** relatives notamment à vos employés ou à vos fournisseurs : gestion RH, listing du personnel, planning, tableau d'astreinte, etc..

Zoom sur les données de santé

Les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne.

Cette définition comprend donc les informations relatives à une personne physique ou identifiable :

■ **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.

■ 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.

■ Concernant par exemple, **une maladie, un traitement médicamenteux, 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 (médecin, autre professionnel de santé, d'un hôpital).

Les données à caractère personnel gérées dans vos établissements

Données de santé par nature	Croisement de données devenant des données de santé	Données de santé en raison de leur utilisation
Dossier médical du patient, antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, handicap...	Permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne : croisement d'une mesure de poids avec d'autres données, etc.	Utilisation des données personnelles à des fins médicales

CNIL.
Pour aller plus loin :
https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante

Qui est responsable de traitement au sein d'un établissement de santé ?

Le responsable de traitement est une personne physique ou morale, autorité publique, service ou autre organisme, juridiquement responsable, qui détermine la finalité et les moyens du traitement : cette qualification implique des responsabilités et des sanctions en cas de non-respect de ses engagements.

La finalité est l'objectif principal pour lequel le traitement est réalisé : elle doit être déterminée, explicite et légitime.

Les moyens du traitement désignent les mesures mises en œuvre pour atteindre cette finalité : équipement, matériel informatique, logiciels, services associés, le budget, le personnel…

Un co-responsable du traitement peut intervenir lorsque les finalités et les moyens du traitement sont propres à deux entités ou plus. Un contrat est alors passé pour définir les droits et les obligations réciproques de chaque responsable de traitement. Le responsable de traitement est amené à interagir avec les fournisseurs, les tiers et autres acteurs intervenant dans la mise en œuvre du traitement.

Par exemple, le responsable de traitement pour **la gestion des effectifs non médicaux** est l'établissement de santé même si la Direction des Ressources Humaines reste en charge de la mise en œuvre du traitement.

Chaque traitement de données à caractère personnel est mis en œuvre sous la responsabilité d'un responsable de traitement.

Le cas des GHT : qui est le responsable de traitement ?

Selon la nature des traitements, leurs finalités, l'organisation retenue au sein du GHT et dès lors qu'ils déterminent conjointement les finalités et les moyens du traitement, l'établissement support et établissements parties au GHT sont responsables conjoints de traitement (ex : dossier médical partagé, traitement utilisé pour le laboratoire commun de biologie médicale, traitement utilisé pour la pharmacie commune, etc.). **Dans ce cas, il est nécessaire de formaliser la coresponsabilité par voie d'accord.**

L'accord de coresponsabilité peut prendre la forme d'une convention ad hoc. Il peut également être formalisé dans les documents constitutifs supports du GHT (convention constitutive, règlement intérieur du GHT) ou encore au niveau du registre des traitements.

La coresponsabilité de traitement entre les établissements parties au GHT, selon la nature du traitement et sa finalité, peut donner lieu à l'accomplissement de nouvelles formalités auprès de la CNIL.

Le délégué à la protection des données personnelles appelé aussi DPO (Data Protection Officer)

2 - Rôle et missions du DPO

Pour piloter la gouvernance des données personnelles et protéger les droits fondamentaux des personnes concernées (patients, personnels, agents…), vous aurez besoin d'un véritable chef d'orchestre : le délégué à la protection des données personnelles. Le DPO doit connaître les caractéristiques-clés de son établissement pour pouvoir adapter ses actions.

Les missions du DPO (La fonction du CIL n'existe plus depuis le 25 mai 2018. Le CIL peut devenir le DPO, mais ce n'est pas obligatoire)

Les missions prévues par le RGPD		Missions supplémentaires définies dans l'organisation de chaque établissement	
Informer et conseiller avant toute mise en œuvre d'un nouveau traitement	Sensibiliser les collaborateurs aux problématiques de protection des données personnelles	Contrôler la mise en œuvre et l'application des règles du RGPD	Le DPO travaille avec le directeur d'établissement et les services concernés pour mettre en place la conformité, avec l'action des responsables de traitements. Ceux-ci sont clairement désignés et responsabilisés
Maintenir à jour le registre des traitements	Veiller au droit d'accès, de rectification et d'opposition des individus (gestion des réclamations reçues)	Vérifier le traitement des demandes de l'autorité de contrôle	
Réaliser un bilan annuel de ses activités	Point de contact de l'autorité de contrôle sur les traitements		

Le DPO peut être interne ou externe à l'établissement et mutualisé entre plusieurs établissements. Pour réunir l'ensemble des compétences attendues et soutenir le DPO, certains établissements ont choisi de créer un comité ou une cellule appelée à se réunir régulièrement regroupant plusieurs catégories de personnes : le DPO, le RSSI, un juriste, un médecin, du temps de secrétariat, etc.

La désignation d'un délégué est obligatoire pour :

- **Les autorités ou les organismes publics**
- **Les organismes dont l'activité de base consiste à traiter des données sensibles à grande échelle** (ex: données de santé, génétiques, etc.)

CNIL.

Pour désigner son DPO :
https://www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo

Comment choisir votre DPO ?

2 - Rôle et missions du DPO

Il est probable que les délégués à la protection des données désignés auprès de la CNIL dès mai 2018 soient d'anciens CIL confirmés dans leur position et pour les nouveaux entrants, des personnes issues des métiers de la sécurité informatique, du droit, de la gestion du risque, ayant reçu les formations complémentaires nécessaires.

Une position stratégique au sein de la hiérarchie	Le DPO doit être en mesure de de faire respecter la réglementation et de remonter l'importance des sujets de données personnelles à la direction
Indépendance	Le DPO ne doit pas être en position de conflit d'intérêt et doit agir indépendamment des personnes qui définissent les traitements
Expertises juridique	Le DPO doit être en mesure de comprendre et de s'approprier le cadre juridique s'appliquant (RGPD, loi Informatique et Libertés, dispositions spécifiques du code de la santé publique, etc.)
Expertises IT	La gestion des données repose sur des applications et des infrastructures IT que le DPO doit maitriser
Intégration aux processus	Le DPO doit identifier les nouveaux cas et anticiper les non conformités et les intégrer au plus vite. Il doit être associé au projet en amont. Les services doivent faire une remontée d'information auprès du DPO.

Le cas des GHT

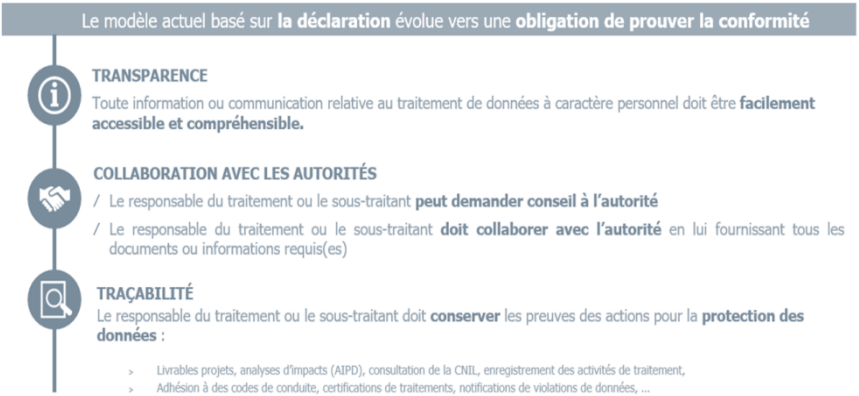
Depuis le 25 mai 2018, date d'application du règlement européen relatif à la protection des données, chaque établissement partie au GHT doit disposer d'un délégué à la protection des données : ce délégué peut être interne ou externe à l'établissement. Par ailleurs, le délégué à la protection des données peut être mutualisé au niveau du GHT c'est-à-dire désigné par plusieurs établissements parties.

Le RGPD : une logique de responsabilisation des acteurs

Le responsable de traitement met en œuvre des mesures techniques et organisationnelles appropriées afin d'être en mesure de démontrer et garantir que le traitement est effectué conformément au RGPD. Ces mesures sont réexaminées et actualisées si le DPO et le responsable de traitement le jugent nécessaire.

Alors que la règlementation nationale reposait jusqu'alors, sur la notion de «formalités préalables» (déclarations, autorisations, engagements de conformité) **le règlement européen repose lui sur une logique de conformité, dont les acteurs sont responsables.**

La documentation interne doit permettre d'attester de la conformité aux grands principes du RGPD (licéité et transparence, minimisation des données, respect des droits, etc.). Il faudra désormais tenir à jour une documentation interne afin de pouvoir rendre compte à la CNIL en cas de contrôle : registre (cf. page suivante), mentions d'information, preuves du recueil du consentement, contrats avec les sous-traitants.



Attention, l'obligation de prouver la conformité ne met pas fin aux demandes d'autorisations (celles-ci ne concernant que des situations très ciblées)

La démarche induite par cette obligation de prouver la conformité au RGPD peut être comparée à une démarche ISO. En effet, les établissements devront mettre en place un socle de processus, décrit dans des procédures, qui permet l'identification, la collecte, le stockage et le maintien en conditions opérationnelles des preuves.

Responsabiliser les acteurs à travers la tenue d'un registre des activités de traitements

Pour recenser l'ensemble des traitements de données à caractère personnel, l'établissement s'appuie sur un registre. Celui-ci permet de cartographier et formaliser l'ensemble de ces traitements de données à caractère personnel gérés dans son établissement. Il est recommandé que le DPO en assure la création, la tenue et notamment la mise à jour.

➢ Que doit contenir le registre des traitements ?

1. Le **nom et les coordonnées du responsable du traitement** et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement, du délégué à la protection des données et du ou des sous-traitant intervenant pendant le traitement.
2. Les **finalités** du traitement
3. Une **description des catégories de personnes** concernées et des catégories de **données** à caractère personnel
4. Les **catégories de destinataires** auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales
5. **Le cas échéant, les transferts de données à caractère personnel vers un pays tiers** ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale, des services traitant des données, etc.
6. Dans la mesure du possible, **les délais prévus pour l'effacement** des différentes catégories de données. Le dossier médical doit être conservé 20 ans après sa dernière consultation (dossier actif)
7. Dans la mesure du possible, **une description générale des mesures de sécurité techniques et organisationnelles**

➢ Qui doit renseigner le registre des traitements ?

En vertu de l'article 30, paragraphes 1 et 2, c'est au responsable du traitement, ou au sous-traitant, de tenir le registre. En revanche, cette mission peut être confiée au DPO mais ce n'est pas une obligation. **Le DPO doit s'assurer de la mise en œuvre du recensement de l'ensemble des traitements identifiés au sein de son établissement**. Il s'organise donc avec les services ou les responsables de traitement pour renseigner le registre.

Que sont les analyses d'impact sur la vie privée (AIPD)* ?

L'analyse d'impact sur la protection des données est un outil important pour la responsabilisation des organismes : elle les aide non seulement à construire des traitements de données respectueux de la vie privée, mais aussi à démontrer leur conformité au RGPD.

Quand faut-il mener une étude d'impacts ?

Lorsque les opérations de traitement sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, notamment les cas suivants :

- Evaluation systématique et approfondie d'aspects personnels sur la base de laquelle sont prises des décisions à l'égard des personnes physiques,
- Traitement à grande échelle de catégories particulières de données, dont les données de santé,
- Traitement de données relatives à des populations vulnérables.

L'AIPD est nécessaire pour les traitements à risque élevé. On considère que c'est le cas si 2 critères dans la liste des 9 critères définis par le G29 sont remplis (voir cette liste à l'adresse : https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-dpia)

Nous vous recommandons également le logiciel CNIL permettant aux acteurs de se poser les bonnes questions et de formaliser leurs études d'impact :
Les AIPD devront être suivies par le DPO en collaboration avec les services concernés ainsi que la DSI. La consultation de la CNIL n'est pas systématique pour les AIPD.

CNIL.

L'outil mis en place par la CNIL permettra aux acteurs de se poser les bonnes questions et de formaliser leur étude d'impacts : https://www.cnil.fr/fr/outil-pia-telechargez-et-

Quand réaliser une AIPD * ?

Vous pouvez vous référer aux deux listes élaborées par la CNIL : https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-dpia

**Appelé aussi DPIA et PIA (Privacy Impact Assessment)*

Quel contrat avec les sous-traitants ?

Lorsqu'un traitement est effectué par un sous-traitant tel qu'un prestataire de service informatique ou un prestataire proposant un service impliquant de traiter les données pour le compte du responsable de traitement, celui-ci doit présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD.

Le sous-traitant est : « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

La gestion des relations entre les acteurs d'un traitement implique de :

- Demander au sous-traitant quelle est **sa politique en matière de protection des données** à caractère personnel ;
- **Documenter les instructions données** au sous-traitant en matière de sécurité et de confidentialité des données ;
- D'élaborer un **contrat** ou des contrats types à conclure entre les différents acteurs mentionnant les obligations respectives des parties ;
- D'effectuer une **revue des contrats existants conclus** avec les sous-traitants pour vérifier si les **mentions obligatoires** y figurent et, à défaut, les intégrer par voie d'avenant ou lors du renouvellement du contrat pour qu'ils soient conformes au RGPD.

CNIL.

Le guide du sous-traitant de la CNIL propose un exemple de clauses de sous-traitance que les acteurs peuvent compléter en fonction de leur situation : https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

Le RGPD renforce le contrôle par les usagers de leurs données personnelles

Le RGPD confirme les droits déjà prévus par la Loi Informatique et Libertés (LIL) et crée de nouveaux droits pour les citoyens. Le RGPD améliore la transparence en renforçant les exigences en terme d'information des usagers sur l'utilisation faite de leurs données et en leur facilitant l'accès à ces informations.

Confirmation des droits prévus par la LIL	Nouveautés
• **Droit à l'information** • **Droit d'accès aux données** • **Droit de rectification** • **Droit à l'oubli** • **Droit d'opposition** • **Droit à la réclamation**	• **Renforcement de l'information des usagers dont les données sont collectées (toutes les mentions de l'article 13 ne sont pas reprises)** ✓ Sur le droit d'exercer une réclamation ✓ Sur les coordonnées du DPO ✓ Sur l'intérêt légitime du responsable de traitement ✓ Sur le droit à l'effacement ✓ Sur le droit d'opposition de la personne • **Droit à la limitation du traitement (art.18)** • **Droit à la portabilité des données (art.20)** ✓ ce droit ne s'exerce que pour les traitements fondés sur le consentement ou l'exécution d'un contrat • **Elargissement des cas de notification des failles de sécurité (art.34)** • **Droit la réparation (art.82)**

Les nouvelles mentions d'information, les procédures mises en place pour répondre aux droits des personnes devront être intégrées dans la documentation de l'établissement afin de bien informer les patients de votre établissement (livret d'accueil, service des admissions, secrétariats médicaux).

Le RGPD renforce le contrôle par les usagers de leurs données personnelles

Le RGPD réaffirme également le droit à l'information et le droit d'accès des patients et de tout autre personne concernée par le traitement de données personnelles en établissement de santé (employés, fournisseurs, etc.)

Droit à l'information

Quiconque met en œuvre un fichier ou un traitement de données à caractère personnel est **obligé d'informer la personne** qui fait l'objet de ce traitement de données personnelles, notamment :

- De l'objectif de la collecte d'informations
- De son caractère obligatoire ou facultatif
- L'identité du responsable du traitement
- La durée de conservation
- Des destinataires des informations
- Des droits reconnus à la personne
- Des éventuels transferts de données vers un pays hors de l'Union européenne
- **…**

L'information doit être claire et adaptée au public concerné.

Droit d'accès aux données

Les personnes concernées peuvent demander directement au responsable d'un fichier s'il détient des informations sur eux et demander à ce qu'on leur communique l'intégralité de ces données. L'exercice du droit d'accès permet de contrôler l'exactitude des données et si besoin de les faire rectifier ou effacer.

Il existe des dispositions spécifiques dans le code de la santé publique pour l'accès des usagers à leur dossier médical.

CNIL.

Pour aller plus loin

Modèles de mention d'informations :

https://www.cnil.fr/fr/modeles/mention

Sécurisez les données personnelles en votre possession

Les mesures nécessaires doivent être prises pour assurer au mieux la sécurité des données à caractère personnel en votre possession afin de garantir au minimum les risques de pertes de données ou de piratage

Les bonnes pratiques à avoir

Certains réflexes doivent être essentiels :

- **Mises à jour** de vos antivirus et logiciels
- Changement régulier et utilisation **de mots de passe complexes**
- **Chiffrement des données dans certaines situations**

En cas de perte ou vol d'un outil informatique, L'accès à son contenu en sera rendu plus difficile pour toute personne non autorisée à l'utiliser.

Les bonnes questions à se poser pour évaluer rapidement le niveau de sécurité de votre établissement, notamment :

- **Les accès aux locaux** sont-ils sécurisés ?
- **Des profils distincts** sont-ils créés selon les besoins des utilisateurs pour accéder aux données ?
- **Une procédure de sauvegarde et de récupération de données régulièrement testée** en cas d'incident a-t-elle été mise en place ?
- **les règles de sécurité fixées par la politique générale de sécurité des systèmes d'information de santé (PGSSI-S)** sont-elles respectées ?

En cas de violation de données (des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées, etc.) **vous devez le signaler à la CNIL, et à la personne concernée, dans les meilleurs délais (au maximum sous 72h) si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées** :
https://notifications.cnil.fr/notifications/index

Le signalement de tout incident de sécurité informatique est obligatoire et doit être déclaré sur : https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil

Pour aller plus loin :

Mémento de cybersécurité réalisé par la DGOS : http://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/sih/article/memento-de-cybersecurite

Guide sécurité CNIL :
https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

☑ POUR AGIR : mémo-quizz “RGPD – êtes-vous prêt ?” 1/3

Le principe du mémo-quizz est très simple : il vous suffit de cocher les exigences qui vous semblent remplies au sein de votre établissement. Tout ce qui n’est pas coché doit donner lieu, sans tarder à une action.

Les 5 étapes ci-dessous seront abordées :

Désigner un pilote

Cartographier les traitements

Gérer les risques des traitements de données à caractère personnel susceptibles

Organiser les processus internes

Documenter la conformité

Désigner un pilote

- ❑ Le DPO a les compétences requises (techniques, juridiques, savoir- faire, etc.)
- ❑ Le DPO dispose des moyens nécessaires
- ❑ Le DPO peut agir en toute indépendance
- ❑ Le DPO est libre de tout conflit d’intérêt

Cartographier les traitements

- ❑ Le DPO a organisé le recensement précis de vos traitements de données à caractère personnel pour l'élaboration d'un registre des traitements
- ❑ Sur la base de ce registre, le DPO a identifié et vous a présenté les actions à mener pour conformer votre établissement aux obligations actuelles et à venir. Il a priorisé ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes

Gérer les risques des traitements de données à caractère personnel susceptibles d'engendrer des risques élevés pour la vie privée des personnes

- ❑ Le DPO a identifié les points d’attention des traitements de votre établissement nécessitant une vigilance particulière : certains types de données traitées, traitements des données à grande échelle, etc.
- ❑ Le DPO a identifié des traitements de données à caractère personnel susceptibles d'engendrer des risques élevés pour la vie privée, des AIPD pour ces traitements sont prévues.

Organiser les processus internes

- ❑ La prise en compte de la protection des données a été mise en place dès l’intégration des projets
- ❑ L’établissement sensibilise et organise la remontée d’informations en proposant des plans de formation et de communication
- ❑ L’établissement peut, à tout moment, répondre et traiter les réclamations et les demandes des personnes concernées quant à l’exercice de leurs droits

Documenter la conformité

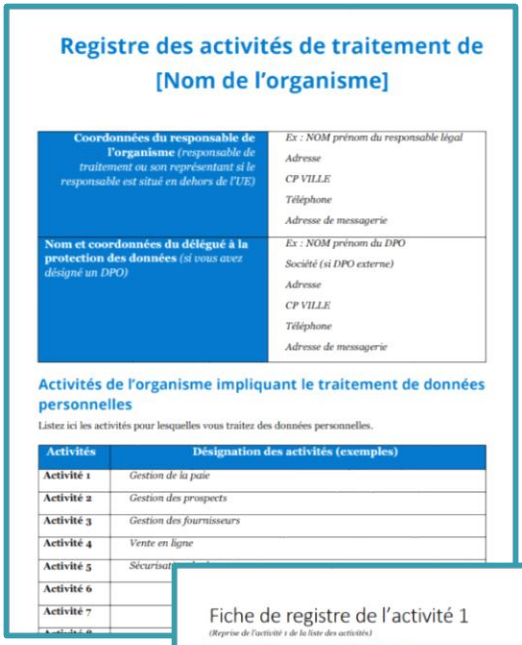
- ❑ La documentation sur les traitements de données à caractère personnel est tenue à jour : registre de traitements, AIPD, encadrement des transferts, etc.
- ❑ Les documents relatifs à l’information des personnes existent : les mentions d’information, les modèles de recueil de consentement des personnes concernées (ou de refus)
- ❑ Les procédures pour l’exercice des droits sont mises en place
- ❑ L’ensemble des documents définissant rôles et responsabilités des acteurs : contrats avec les sous-traitants, procédures internes en cas de violation de données, mentions d’information, etc.

6 - Liens vers la documentation existante

De nombreux documents et outils à destination des établissements de santé sont également disponibles sur les sites internet de la CNIL et de l'ASIP-Santé :

- ✓ **Une rubrique sur les données de santé sur le site de la CNIL :** https://www.cnil.fr/fr/sante
- ✓ **Un guide de la sécurité des données personnelles rédigé par la CNIL** : https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles
- ✓ **Une fiche synthétique pour les établissements de santé rédigée par l'ASIP- Santé** : https://esante.gouv.fr/sites/default/files/media_entity/documents/rgpd-fiche-1.pdf
- ✓ **Une fiche synthétique pour se préparer à une mise en conformité** : https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes
- ✓ **Un guide sur le sous- traitant :** https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf
- ✓ **Le portail d'information sur la sécurité numérique dans le secteur santé :** www.cyberveille-sante.gouv.fr
- ✓ **formation en ligne de la CNIL ouverte à tous (MOOC) :** https://www.cnil.fr/fr/la-cnil-lance-sa-formation-en-ligne-sur-le-rgpd-ouverte-tous

Modèle de fiche et de registre proposé par la CNIL



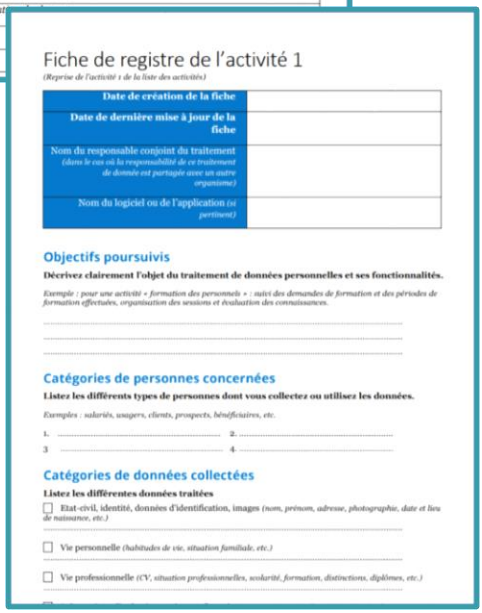
Registre des activités de traitement de [Nom de l'organisme]

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

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 (exemples)
Activité 1	*Gestion de la paie*
Activité 2	*Gestion des prospects*
Activité 3	*Gestion des fournisseurs*
Activité 4	*Vente en ligne*
Activité 5	*Sécurisat…*
Activité 6	
Activité 7	



Fiche de registre de l'activité 1

(Reprise de l'activité 1 de la liste des activités)

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

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.

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. …… 2. ……

3 …… 4 ……

Catégories de données collectées

Listez les différentes données traitées

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

……

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

……

☐ Vie professionnelle *(CV, situation professionnelles, scolarité, formation, distinctions, diplômes, etc.)*

……

Le format du registre est libre: Excel, Word …

CNIL.

Les outils pour vous aider :

https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

Mini-glossaire

sigle	*désignation*
ACSS	Accompagnement cybersécurité des structures de santé
AQSSI	Autorité qualifiée pour la sécurité des systèmes d'information.
CIL	Correspondant informatique et liberté
DPD	Délégué à la protection des données personnelles
DPI	Dossier patient informatisé
DPO	Data protection officer (idem DPD) – Appellation retenue par la CNIL
EIPD	Etude d'impact sur la protection des données (idem EIVP)
EIVP	Etude d'impact sur la vie privée
GHT	Groupement hospitalier de territoire
HDS	Hébergeur de données de santé
PGSSI-S	Politique générale de sécurité du système d'information de santé
DPIA	Data protection impact assesment (idem EIVP)
RGPD	Règlement général européen sur la protection des données
RSSI	Responsable sécurité du système d'information
SI / SIH	Système d'information / Système d'Information Hospitalier

Les sites institutionnels de référence :

ANSSI	Agence Nationale de la sécurité des systèmes d'information	www.ssi.gouv.fr
ASIP Santé	Agence française de la santé numérique	esante.gouv.fr
CNIL	Commission Nationale de l'Informatique et des Libertés	www.cnil.fr
DGOS	Direction Générale de l'Offre de Soins	solidarites-sante.gouv.fr - lien DGOS
DSSIS	Délégation à la stratégie des systèmes d'information de santé	solidarites-sante.gouv.fr - lien DSSIS
HAS	Haute autorité de santé	has-sante.fr
FSSI	Fonctionnaire de sécurité des systèmes d'information	solidarites-sante.gouv.fr - lien FSSI

Remerciements

Ce « Mémento » a été élaboré en s'appuyant sur un groupe de travail associant des RSSI, DPO d'établissement ou de région, médecin et juristes de l'ASIP , de la CNIL et des experts et représentants du ministère des solidarités et de la santé :

Julie	CHABROUX	Chargé de mission - DSSIS
Jean-Christophe	DAYET	Chargé de mission - DSSIS
Florence	EON	Directrice juridique - ASIP Santé
Nicole	JANIN	Directrice des affaires médicales - ASIP Santé
Jean-Michel	KERMARREC	Délégué à la Protection des Données - CHU Montpellier
Eve	LE COQ	Conseillère juridique - DGOS/SR1
Auriane	LEMESLE	Référente régionale SSI - GCS e-Santé Pays de la Loire
Philippe	LOUDENOT	FSSI - HFDS ministère
Lorraine	MAISNIER-BOCHÉ	Juriste – ASIP Santé
Marjorie	MENAPACE	Juriste - CNIL - Service de la santé
Stéphane	PASQUIER	FSSI adjoint- HFDS ministère
Sandrine	PAUTOT	Adjointe à la Sous-directrice - DGOS/SR
Stéphanie	SAULNIER	Juriste - CNIL - Service de la santé
Philippe	TOURRON	RSSI - AP/HM
Michel	RAUX	Adjoint à la Cheffe de Bureau DGOS/PF5

Il a également bénéficié des nombreux échanges informels qui animent le « Club des RSSI Santé » dont les réunions régulières favorisent les partages d'expériences et permettent d'assurer une véritable veille technologique.

WWW.SOLIDARITES-SANTE.GOUV.FR/SIH

DIRECTION
GÉNÉRALE
DE L'OFFRE
DE SOINS