

Un Kit RGPD opérationnel et adaptable

Accompagnement dans la mise en conformité au RGPD

Table des matières

1. Introduction

Pourquoi un kit RGPD pour les CPTS ?

Le rôle du Guichet CPTS Occitanie

Pourquoi parle-t-on autant de RGPD ?

Le RGPD, concrètement ?

Pourquoi s'y intéresser concrètement ?

Cybersécurité et RGPD : une même logique de protection

2. Comment utiliser le kit RGPD

3. Contenu du pack incontournable et pack complémentaire

a) Pack incontournable

b) Pack complémentaire

4. Ressources complémentaires

5. Un accompagnement dédié

1. Introduction

Pourquoi un kit RGPD pour les CPTS ?

La mise en conformité au Règlement Général sur la Protection des Données (RGPD) est aujourd'hui un enjeu incontournable pour toutes les CPTS.

Dans le cadre de leurs missions de coordination, de prévention et d'appui à l'accès aux soins, les CPTS manipulent quotidiennement des données à caractère personnel, souvent sensibles : données d'adhérents, de partenaires, de salariés, et parfois de patients, qui nécessitent une vigilance renforcée en raison de leur sensibilité (données de santé).

Afin de faciliter cette démarche, le Guichet CPTS Occitanie a conçu un kit RGPD, élaboré avec l'appui de Délégués à la Protection des Données (DPO).

👉 L'objectif de ce kit est de fournir aux CPTS une base documentaire conforme aux exigences du RGPD, à adapter en fonction des traitements, de l'organisation et des pratiques propres à chaque CPTS.

⚠ Ce kit constitue une base de travail et ne garantit pas, à lui seul, la conformité RGPD de la CPTS.

Le rôle du Guichet CPTS Occitanie

Le Guichet CPTS Occitanie propose ce kit RGPD à titre d'outil d'accompagnement et de sensibilisation.

Chaque CPTS agit en tant que responsable de traitement pour les données qu'elle utilise. À ce titre, elle demeure responsable de la conformité de ses traitements au RGPD et de l'adaptation des documents proposés à sa situation spécifique.

Le Guichet CPTS n'intervient ni en qualité de responsable de traitement, ni en tant que délégué à la protection des données (DPO) des CPTS.

Pourquoi parle-t-on autant de RGPD ?

C'est une réaction que l'on entend souvent : « *Encore une règle de plus, un document à remplir, un tableau à tenir à jour... Avec tout ce qu'on a déjà à faire dans une CPTS, c'est le dernier sujet qu'il nous manquait.* »

Et pourtant. Le RGPD n'est pas une contrainte administrative supplémentaire.

C'est avant tout un outil de protection des personnes, un cadre de sécurisation des pratiques, et, un levier de confiance entre professionnels, partenaires et usagers.

Le RGPD, concrètement ?

Le RGPD encadre la manière dont nous collectons, stockons et partageons les données à caractère personnel. Et cela concerne toutes les CPTS, car elles manipulent chaque jour :

- des données d'adhérents et de partenaires (professions, coordonnées, cotisations),
- des données de salariés et prestataires,
- et parfois des données de patients dans le cadre d'actions de prévention ou de coordination.

Le RGPD s'applique quel que soit le support utilisé :

- supports papier (formulaires, feuilles de présence, questionnaires),
- supports numériques (fichiers, outils collaboratifs, messageries, sites web).

Pourquoi s'y intéresser concrètement ?

Respecter le RGPD, c'est avant tout faire preuve de bon sens et de professionnalisme.

Cela permet de :

- protéger les données des personnes accompagnées et des professionnels impliqués,
- garantir la confidentialité des échanges,
- prévenir les erreurs et incidents (perte de données, envoi par erreur, mauvais partage),
- éviter les sanctions de la CNIL,
- et surtout renforcer la crédibilité et la confiance accordée à la CPTS.

Cybersécurité et RGPD : une même logique de protection

La conformité RGPD passe aussi par des pratiques numériques sécurisées.

Chaque CPTS peut réduire significativement les risques en adoptant quelques bons réflexes de cybersécurité, parmi lesquels :

- séparer les usages personnels et professionnels,
- utiliser des mots de passe robustes et uniques,
- maintenir les ordinateurs et logiciels à jour,
- utiliser des messageries et outils sécurisés (MSSanté, Médimail, SPICO...),

- sauvegarder régulièrement les données,
- être vigilant face aux emails, liens ou pièces jointes suspects,
- verrouiller systématiquement sa session en cas d'absence.

👉 Ces gestes simples complètent la démarche RGPD et protègent à la fois l'activité de la CPTS et les données traitées.

2. Comment utiliser le kit RGPD ?

Le kit est conçu pour être souple et adaptable. Il est organisé en deux niveaux complémentaires, permettant à chaque CPTS d'avancer à son rythme selon sa maturité et son organisation.

Chaque structure peut utiliser tout ou partie des documents proposés : il est tout à fait possible de s'appuyer sur certains modèles du kit, d'en adapter quelques-uns, ou d'aller plus loin sans nécessairement mobiliser l'ensemble des documents.

Il est structuré en **deux niveaux complémentaires** :

- un **pack incontournable**, regroupant les documents indispensables,
- un **pack complémentaire**, pour aller plus loin dans la structuration et la gouvernance des données.



3. Contenu du pack incontournable et pack complémentaire

a) Pack incontournable

Ce premier niveau regroupe les **documents essentiels** pour toute CPTS.

Le RGPD repose sur deux piliers :

- Responsabilité → documentation interne.
- Transparence → information des personnes concernées.

Sensibilisation

Ces supports ont pour objectif d'aider la CPTS à comprendre les principes du RGPD et les enjeux de cybersécurité.

Ils permettent d'acculturer les équipes, de mieux identifier les risques, et, de structurer la démarche.

Ils ne constituent pas des obligations formelles, mais facilitent la mise en conformité.

- **RGPD et CPTS**
- **Cybersécurité et CPTS**

Documents internes

Ces documents structurent l'organisation interne de la CPTS. Ils doivent être conservés en interne et tenus à jour. Ils ne sont pas destinés à être publiés.

- **Registre des traitements** : Document central recensant l'ensemble des traitements de données réalisés. Il comprend une trame de registre basée sur le modèle de la CNIL, ainsi qu'un exemple de fiche complétée (gestion des adhérents) à adapter selon les activités de la CPTS. Chaque traitement fait l'objet d'une fiche, organisée par typologie d'activité et précisant notamment la finalité et la base légale associée. Le registre doit être organisé par finalité principale (art. 30 RGPD).

Objectif : structurer et démontrer la conformité.

- **Charte d'utilisation des systèmes d'information** : Règles internes relatives à l'usage des outils numériques.

Objectif : diffuser une culture commune de sécurité et de confidentialité.

- **Gestion des demandes d'exercice de droits et des violations de données :**

Document interne présentant les obligations de la CPTS et les réflexes à adopter en cas de demande de droits ou d'incident de sécurité.

Objectif : comprendre les situations concernées et savoir réagir de manière adaptée, en complément des outils de suivi proposés dans le pack complémentaire.

Documents externes

Ces documents sont destinés aux adhérents, partenaires, salariés ou usagers. Ils garantissent la transparence exigée par le RGPD. Certains doivent être accessibles publiquement (site internet).

- **Formulaire d'adhésion :** Informer les adhérents sur l'utilisation de leurs données et recueillir leur consentement.

Objectif : garantir la transparence dès la collecte.

- **Mentions légales :** Informations obligatoires figurant sur le site internet ou les supports de communication.

Objectif : identifier clairement le responsable de traitement.

- **Politique de confidentialité :** Présentation claire des modalités de collecte, d'utilisation et de protection des données.

Objectif : informer les usagers et partenaires.

- **Politique de gestion des cookies :** Encadrement de l'utilisation des traceurs sur le site web.

Objectif : respecter les règles de consentement.

b) Pack Complémentaire

Ce second niveau s'adresse aux CPTS souhaitant aller plus loin dans leur démarche RGPD.

Il comprend notamment :

- **Registre des sous-traitants** : Document permettant d'identifier les prestataires intervenant pour le compte de la CPTS et susceptibles de traiter des données personnelles.

Objectif : encadrer les relations avec les sous-traitants et vérifier les garanties en matière de sécurité, de confidentialité et de conformité au RGPD.

- **Procédures internes** (violations de données, droits des personnes, sécurité) : Document décrivant les démarches à suivre en cas de demande d'exercice de droits ou d'incident de sécurité, ainsi que les règles d'usage des outils et des accès.

Objectif : formaliser les réflexes à adopter, sécuriser les pratiques et garantir une gestion cohérente des demandes et des incidents.

- **Registre des violations de données** : Document permettant de consigner les incidents de sécurité impliquant des données personnelles (perte, accès non autorisé, envoi par erreur, etc.).

Objectif : assurer la traçabilité des incidents et répondre aux obligations du RGPD en matière de notification.

- **Une AIPD - Ma CPTS doit-elle réaliser une analyse d'impact ?** : Document pédagogique présentant l'analyse d'impact relative à la protection des données (AIPD), ses objectifs et les situations dans lesquelles elle peut être requise en fonction du niveau de risque des traitements.

Objectif : aider la CPTS à évaluer les risques liés à ses traitements et à déterminer, au cas par cas, si la réalisation d'une AIPD est nécessaire.

- **Charte d'usage de l'intelligence artificielle** : Document définissant les règles et bonnes pratiques d'utilisation des outils d'intelligence artificielle au sein de la CPTS.

Objectif : encadrer les usages, prévenir les risques liés aux données et garantir un usage conforme au RGPD.

👉 Ce pack renforce la traçabilité, la sécurité et la gouvernance des données.

4. Ressources complémentaires

MOOC CNIL : <https://atelier-rgpd.cnil.fr/login/index.php>

Webinaire guichet CPTS RGD

Webinaire guichet CPTS Cybersécurité

FAQ guichet CPTS Cybersécurité

FAQ guichet CPTS ma CPTS doit-elle désigner un DPO ?

5. Un accompagnement dédié

Le kit RGD est conçu pour être autonome, évolutif et opérationnel, tout en favorisant le partage d'expériences entre CPTS. Il permet aux CPTS d'initier ou de structurer leur démarche de mise en conformité en toute autonomie.

Comprendre et s'appropriier le kit : Guichet CPTS Occitanie

Le Guichet CPTS accompagne les structures dans :

- *la compréhension des enjeux du RGD,*
- *la prise en main des outils du kit,*
- *l'identification des premières priorités dans la mise en conformité.*

Cet accompagnement constitue un premier niveau d'appui, sans se substituer à une expertise juridique ou à un délégué à la protection des données.

Aller plus loin dans la mise en conformité : FACS Occitanie *La FACS Occitanie propose un accompagnement spécialisé, notamment :*

- *l'aide à la rédaction et à l'adaptation des documents,*
- *l'analyse des traitements,*
- *la structuration d'une démarche de conformité RGD complète.*