**Fiche pratique : outils de mise en conformité RGPD**

Le Règlement général sur la protection des données (RGPD) applicable depuis le 25 mai 2018 prévoit un certain nombre d’outils que le responsable de traitements (RT) doit mettre en place afin de pouvoir démontrer la conformité des traitements de données personnelles mis en place et ce tout au long de leur cycle de vie (principe d’*Accountability)*. Par ailleurs, le RGPD impose au RT de prendre les mesures nécessaires afin d’assurer la conformité des traitements de données personnelles dès leur conception (principe de *Privacy by design)*.

Ces obligations s’inscrivent dans une logique de responsabilisation des acteurs qui pèsent sur l’ensemble des RT y compris ceux relevant du secteur de l’inclusion sociale.

Cette fiche pratique destinée aux structures de l’inclusion sociale qu’elles soient du secteur de l’Accueil, Hébergement et Insertion (AHI), de l’Insertion par l’Activité Economique (IAE) ou du Dispositif National d’Accueil (DNA) a vocation à synthétiser le cadre juridique des outils de conformité RGPD et à apporter des pistes de réflexion pratiques pour faciliter leur déploiement.

**Les outils de mise en conformité RGPD en théorie**

***Quel est le cadre juridique général des outils de mise en conformité ?***

C’est le RGPD qui a mis en place les outils de mise en conformité et ce dans en vue de responsabiliser les acteurs. Etant un texte de droit commun, l’encadrement juridique est assez général.

Compte tenu des spécificités du secteur de l’inclusion sociale (traitements de données sensibles de publics en situation de vulnérabilité, échanges de données en interne et externe fréquents), la CNIL a apporté des précisions des principes généraux du RGPD dans le [Référentiel relatif aux traitements de données à caractère personnel mis en œuvre dans le cadre de l’accueil, l’hébergement et l’accompagnement social et médico-social des personnes âgées, des personnes en situation de handicap et de celles en difficulté (« Référentiel Social ») élaboré par la CNIL et publié le 24 mars 2021](https://www.cnil.fr/sites/default/files/atoms/files/referentiel_relatif_aux_traitements_de_donnees_personnelles_pour_le_suivi_social_et_medico-social_des_personnes_agees_en_situation_de_handicap_ou_en_difficulte.pdf).

Ce Référentiel apporte des éclairages notamment s’agissant certains outils de mise en conformité, afin de guider les RT dans leur mise en conformité de leurs activités.

***Que prévoit le RGPD complété par le Référentiel social ?***

* **Abolition des démarches déclaratives auprès de la CNIL**

Comme indiqué précédemment, le principe d’*Accountability* implique que les RT devront mettre en place les mesures nécessaires afin d’assurer une protection optimale des données personnelles traitées. Ils doivent être en mesure de pouvoir démontrer la conformité de leurs traitements à tout moment (formalisée par les outils de mise en conformité).

Dans ce contexte, le système général de déclarations auprès de la CNIL a été aboli (sauf pour certains traitements de données personnelles relatifs à la recherche ou d’études en matière de santé notamment). En contrepartie, le RGPD prévoit des outils de mise en conformité visant à démontrer le respect du principe d’*Accountability.*

* **Mettre en place des outils de mise en conformité RGPD par chaque RT**

Le RGPD prévoit plusieurs outils de mise en conformité obligatoires et facultatifs qui doivent comporter un certain nombre d’informations synthétisées ci-dessous :

|  |  |
| --- | --- |
| **Encadrement général prévu par le RGPD** | **Complément sectoriel apporté par le Référentiel social** |
| **Type d’outil et référence juridique** | **Obligatoire/facultatif** | **Objectifs poursuivis** | **Mentions requises** |
| Registre de traitements (**art. 30 du RGPD)** | Obligatoire | 1.Identification de chaque traitements mis en place et de ses caractéristiques 2.Outil de pilotage et de démonstration de la conformité RGPD | Pour chaque activité de traitements (grande famille de traitements) : **1.L’identité et les coordonnées du RT**2.Les **finalités** du traitement3.Les catégories**de personnes concernées, soit les personnes dont les données sont collectées**4.Les catégories de  **données personnelles** (exemples : identité, situation familiale ..) **5.Les catégories de destinataires** auxquels les données à caractère personnel ont été ou seront communiquées, y compris les sous-traitants auxquels vous recourez6.Les **transferts** de données à caractère personnel vers un pays hors UE 7.Les **durées de conservation** des données8.Une **description générale des mesures de sécurité** techniques et organisationnelles mises en œuvre |  **---** |
| Mentions d’informations **(art. 12 à 14 du RGPD)** | Obligatoire  | Permettre aux personnes concernées de comprendre comment et pourquoi leurs données personnelles sont traitées et de connaitre leurs droits prévus par le RGPD **(principe de transparence)** | 1.Identité et coordonnées du RT2. Finalités de traitements3. Base légale des traitements4.Caractère obligatoire ou facultatif du recueil des données5.Destinataires ou catégories de destinataires des données6.Durée de conservation des données 7.Droits des personnes concernées 8.Coordonnées du délégué à la protection des données de l’organisme, s’il a été désigné, ou d’un point de contact sur les questions de protection des données personnelles 9.Droit d’introduire une réclamation auprès de la CNIL  | Le Référentiel rappelle la règle générale tenant à ce que les personnes concernées soient informées des modalités de traitements de leurs données et de leurs droits au moment de la collecte. Au vu de la vulnérabilité des publics accompagnés/accueillis par les structures de l’inclusion sociale, **le RT doit être particulièrement attentif au respect du principe de transparence en doublant l’information écrite** (au besoin, rédigée en ayant recours à la **méthode « Facile à Lire et à Comprendre »)** d’une **information orale afin de s’assurer de la bonne compréhension des informations communiquées** |
| Analyse d’impact sur la protection des données (AIPD) **(art.35 du RGPD)** | Obligatoires pour certains traitements (analyse au cas par cas à l’aide de critères prévus par le RGPD)**Cf. colonne relative au Référentiel social** | 1.Vise à identifier et évaluer les risques sur la vie privée des personnes concernées issues de traitements de données personnelles pour trouver des moyens de les limiter 2.Outil visant à démontrer la conformité des traitements concernés au RGPD | Pas d’informations ciblées requises mais trois axes doivent figurer dans l’AIPD : 1.Description détaillée du traitement mis en œuvre (aspects techniques et opérationnels) 2.Evaluation de la nécessité du traitement et de sa proportionnalité concernant la vie privée et droits fondamentaux des personnes concernées (aspects juridiques) 3.Etude des risques sur la sécurité des données ainsi que leurs impacts potentiels sur la vie privée pour déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données (aspects techniques) | AIPD obligatoire pour :1.Les traitements de données personnelles relatifs à l’accompagnement social et/ou médico-social des personnes 2.Les traitements de données personnelles relatifs à la prise en charge des personnes mis en œuvre par les établissements de santé ou médico-sociauxPoint d’attention : la liste n’est pas exhaustive. Ces deux traitements ciblés sont identifiés dans le Référentiel car sont très fréquents dans le secteur.  |
| Contrat de sous-traitance **(art.28 du RGPD)** | Obligatoire  | 1.Vise à clarifier la répartition des obligations/responsabilités entre le RT et son sous-traitant (ST)2. Vise à fournir les instructions nécessaires au ST pour qu’ils puissent traiter les données conformément aux directives du RT | Un certain nombre d’obligations juridiques doivent figurer et être adaptées en fonction du contexte : 1.Obligation pour le ST de traiter les données en fonction des instructions documentées fournies par le RT (à formaliser dans l’accord) 2. ST garantie que les personnes traitant les données sont soumises à une obligation de confidentialité 3.ST garantie la sécurité des données 4.ST garantie que le ST ultérieur dans l’exécution conforme du traitement de données personnelles 5.ST a une obligation de coopération avec le RT pour l’exercice des droits des personnes et plus largement pour assurer le respect du RGPD dans l’exécution de ses missions (modalités à formaliser dans l'accord)6.ST met à la disposition du RT les informations nécessaires pour démontrer sa conformité au RGPD et coopère avec ce dernier en cas d’audit réalisé à sa demande ou par ses propres moyens (le cas échéant, les modalités sont à formaliser dans l’accord)7. ST restitue ou supprime les données au choix du RT et détruit toutes les copies éventuelles (modalités à formaliser dans l’accord)  |  |

Dans la logique de documentation de la conformité, le RGPD prévoit aussi d’autres outils de mise en conformité à mettre en place comme le [registre de violation de données](https://www.cnil.fr/fr/les-violations-de-donnees-personnelles). Pour des impératifs de preuve, il est aussi nécessaire d’en formaliser certains. C’est le cas du recueil **explicite** du consentement des personnes concernées nécessaire en cas de collecte de données sensibles (santé, opinions religieuses et politiques…). Pour être conforme, le formulaire de recueil du consentement doit répondre à plusieurs principes prévus par le RGPD (consentement éclairé par exemple).

*Pour aller plus loin sur le consentement :* [*support de sensibilisation relatif au Référentiel social conçu par la Fédération des acteurs de la solidarité*](https://www.federationsolidarite.org/wp-content/uploads/2022/05/Outil-RGPD-relations-avec-les-publics-accompagnesVF.pdf)*,* [*page d’information relative au consentement du site internet de la CNIL*](https://www.cnil.fr/fr/les-bases-legales/consentement)

* **Sanctions en cas d’absence de mise en place des outils**

Le RGPD, à son article 83, prévoit un renforcement des sanctions en cas de violation des obligations du RGPD incluant celles imposant de mettre en place les outils de mises en conformité précités :

* Amende administrative plafonnée à 20 millions d’euros en cas de méconnaissance des obligations concernant l’information des personnes concernées ;
* Amende administrative plafonnée à 10 millions d’euros en cas de méconnaissance des obligations concernant le registre de traitements, l’AIPD et le contrat de sous-traitance.

**Les outils de mise en conformité RGPD en pratique**

Le déploiement des outils de mise en conformité RGPD invite les RT à prévoir/adapter les processus internes existants. Par ailleurs, la CNIL préconise de manière générale, dès qu’il s’agit de mise en conformité RGPD, de construire un plan d’actions.

Afin de vous guider dans son élaboration, voici ci-dessous quelques orientations/bonnes pratiques à mettre en application (avec un focus sur la mise en place d’outils de mise en conformité).

***Capitaliser sur la complémentarité des outils de mise en conformité***

Le registre de traitements comporte toutes les informations requises pour construire les mentions d’information

Les informations contenues dans le registre de traitements vont faciliter la mise en place d’AIPD (lorsqu’elle est requise) puisqu’il compile des éléments généraux sur les traitements de données étudiés

Compte tenu des informations communes à renseigner dans chacun des différents outils précités, il est préconisé d’en tirer profit afin de faciliter leur déploiement.

***Impliquer les acteurs internes/externes pertinents pour déployer les outils de mise en conformité***

**Délégué à la protection des données (DPD/DPO) :** il a pour rôle d’accompagner la structure dans sa mise en conformité au RGPD à tous les stades de la mise en conformité (cartographie des traitements de données, analyse de leur conformité, détermination des actions de mise en conformité et suivi).

**Chefs de service, membre de la direction :** ils auront une vision globale des traitements de données personnelles mis en place dans chaque service/structure qui devront être analysés.

**Les membres du personnel en contact direct avec les personnes concernées**(travailleurs sociaux, secrétaires administratifs, bénévoles …) : elles collectent les données et assurent la gestion quotidienne des traitements de données personnelles des publics accompagnés. Leur implication dans la construction des outils de mise en conformité est indispensable pour comprendre le cadre dans lequel les données sont collectées et traitées (et ainsi analyser leur conformité).

**Personnes concernées :** ce sont les personnes dont les données personnelles sont collectées. S’agissant plus particulièrement des publics accompagnés, leur implication peut être sollicitée par exemple au stade de la conception des mentions d’information ; le Référentiel social insistant sur le caractère compréhensible de ces dernières.

**Services déconcentrés de l’Etat (DDETS, DRETS, ARS …) :** ils ont pour missions d’animer et de coordonner les politiques publiques de l’action sociale. Du côté des structures, elles peuvent être amenées à traiter voire échanger des données personnelles dans le cadre de partenariat avec les services déconcentrés de l’Etat ce qui implique de clarifier les obligations et responsabilités incombant à chacun.

**Partenaires :** dans le cadre des missions découlant de ce partenariat, la structure concernée et son partenaire sont amenés à collecter, traiter et échanger des données personnellesce qui implique de clarifier les obligations et responsabilités incombant à chacun.

**Associations de délégués à la protection des données, fédérations et syndicats professionnels** : ils ont pour rôle d’informer voire d’appuyer les structures dans leur mise en conformité au RGPD notamment via du partage d’expériences ; ce qui peut en effet faciliter la définition de bonnes pratiques.

***Mobiliser les ressources existantes en matière de protection des données***

Outre son rôle d’autorité de contrôle, la CNIL a pour missions d’informer, de conseiller les organismes traitant des données personnelles. Dans ce contexte, elle a conçu différents outils d’accompagnement dans la mise en conformité aussi bien généralistes que sectoriels.

S’agissant des structures de l’action sociale, plusieurs outils CNIL sont pertinents et certains d’entre eux sont spécifiques au secteur (Référentiel social, kit des travailleurs sociaux pour l’accompagnement numérique …).

Pour en savoir plus, cliquez ici [lien vers doc recensant les outils CNIL].

Par ailleurs, la Fédération a également élaborer des documents visant à accompagner les adhérents dans leur mise en conformité RGPD :

* [un support de sensibilisation au RGPD concernant les traitements de données personnelles des publics accompagnés du secteur de l’inclusion sociale (AHI, DNA, IAE …) destiné à toute personne en poste au sein d’une structure du secteur (direction, délégué à la protection des données (DPO/DPD), secrétaire, CIP, travailleurs sociaux…)](https://www.federationsolidarite.org/wp-content/uploads/2022/05/Outil-RGPD-relations-avec-les-publics-accompagnesVF.pdf) ;
* [une foire aux questions sur les traitements de données personnelles liés à la gestion des ressources humaines tirée des remontées d’adhérents en 2021 notamment celles issues du webinaire dédié organisé le 23 novembre 2021;](https://www.federationsolidarite.org/wp-content/uploads/2022/05/RGPD-gestion-des-ressources-humaines-VF.pdf)
* [une foire aux questions sur la sécurisation des données tirée également des remontées d’adhérents de 2021 notamment celles issues du webinaire dédié organisé le 1er décembre 2021 (touchant aussi bien aux traitements de données liés à la gestion interne qu’à ceux liés aux relations avec les publics accompagnés).](https://www.federationsolidarite.org/wp-content/uploads/2022/05/RGPD-securisation-des-donnees-personnelles-VF.pdf)

***Construire avec l’ensemble des parties prenantes la démarche de mise en conformité en adéquation avec vos ressources***

Cette démarche de conformité implique nécessairement deux grandes étapes clés :

* **l’audit de vos activités de traitements de données** personnelles qui vise à recenser tous les traitements de données personnelles de la structure (le [modèle de registre de traitements simplifié (format ODS) de la CNIL](https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement) vous aidera dans cette importante étape) ;
* **l’analyse d’écart des traitements de données personnelles** existant par rapport aux règles de protection des données ;
* **la construction d’un plan d’action de mise en conformité** à l’aide de l’analyse d’écart en priorisant les actions en fonction des risques existants en matière de données personnelles (déploiement/mise à jour de l’information des personnes concernées, régularisation/actualisation des traitements de données sensibles, mise en place/mise à jour des mesures de sécurité des données techniques et organisationnelles, sensibilisation/formation au RGPD des équipes …).

**L’accomplissement de ces étapes impliquent du temps de travail conséquent et des compétences spécifiques. En l’absence de telles ressources internes, les structures peuvent se tourner des organismes proposant des services d’accompagnement à la mise en conformité accomplis par les délégués à la protection des données. Ces services peuvent être mutualisés entre différentes structures permettant de favoriser de l’échange de bonnes pratiques.**