MODULE
Règlement général sur la protection des données -RGPD
REFERENTIEL SOCIAL

La Fédération est co-financée par l'Union européenne

PARTIE 1 – CONTEXTE ET ENJEUX GENERAUX

1. LE CADRE JURIDIQUE
2. LE CADRE INSTITUTIONNEL

La Fédération est co-financée par l'Union européenne

LE CADRE JURIDIQUE (1/2)

- Différents types de normes complémentaires régissent le cadre juridique en matière de protection des données :

Textes obligatoires	Textes de *soft law (application fortement recommandée)*
• **Au niveau européen** : RGPD qui est d'application directe au sein de chaque Etat Membre de l'UE • **Loi Informatique et Libertés (LIL):** loi française régissant sur les sujets pour lesquels le RGPD laisse une marge nationale d'appréciation (ex: fixation à 15 ans du seuil d'âge du consentement des mineurs aux services en ligne, fichiers « répressifs »).	• **Textes visant à clarifier l'interprétation de ceux obligatoires/ apporter des exemples concrets** • **Au niveau européen :** Lignes directrices du Comité européen pour la protection des données (CEPD) : *Ex: Lignes directrices sur les responsables de traitements et sous-traitants* • **Au niveau national :** référentiels, guides et lignes directrices de la CNIL *Ex: Référentiel « secteur social »*

LE CADRE JURIDIQUE (2/2)

Zoom sur les apports principaux du RGPD :

- Application obligatoire pour mettre fin aux disparités d'interprétation de l'ancien cadre juridique européen (directive de 1995)

⇒ Le RGPD forme un socle commun de règles qui remplace le droit national sur plusieurs points majeurs (bases légales, droits des personnes, mesures de sécurité, transfert de données etc.)

- Renforce considérablement les sanctions pouvant être des amendes jusqu'à 20 millions d'euros/ représentant 4% chiffre d'affaires de la personne morale
- Créé une nouvelle autorité de contrôle européenne, le Comité pour la protection des données (CEPD) qui a pour mission notamment de surveiller et garantir la bonne application du RGPD, élaborer des recommandations et des lignes directrices
- Etoffe les droits des personnes en renforçant des droits préexistants (droit à l'information) et en en consacrant de nouveaux (droit à la portabilité des données)
- Responsabilise chaque acteur dès la conception d'un traitement de données ce qui a conduit à la suppression du système de formalités préalables (déclaration/autorisation) de la CNIL

⇒ Désormais, chaque acteur doit assurer la conformité de son traitement **dès son origine et tout au long de son existence et le justifier en cas de contrôle**

PARTIE 1 – CONTEXTE ET ENJEUX GENERAUX

1. Le cadre juridique
2. Le cadre institutionnel

La Fédération est co-financée par l'Union européenne

LE CADRE INSTITUTIONNEL

▶ Missions de la CNIL

Informer et protéger les personnes	• En 2020: • 13 585 plaintes • 3286 vérifications réalisées
Conseiller et accompagner les entreprises/organismes dans la mise en conformité au RGPD	• Elabore aussi des **certifications, référentiels et des études** • **Avis** sur les projets de loi, traitements de données de l'Etat
Contrôler et sanctionner les manquements aux règles de la protection des données	• Sanction **de 100 M€ contre Google** • Sanction **de 75 000 euros** contre une association

La CNIL a pour mission d'accompagner les structures dans leur mise en conformité, donc n'hésitez pas à prendre contact avec eux !
Une permanence DPO est mise en place

PARTIE 2 – LE REFERENTIEL « SOCIAL » (GENERALITES)

1. ENJEUX SOULEVÉS DANS LE SECTEUR SOCIAL
2. QUE RECOUVRE LE RÉFÉRENTIEL SOCIAL?

La Fédération est co-financée par l'Union européenne

ENJEUX SOULEVES DANS LE SECTEUR DE L'INCLUSION SOCIALE

- ► Adaptation de l'accompagnement social à construire :

- ✓ L'accompagnement social des personnes en situation de précarité sociale dans les structures implique **un échange/accès de données personnelles important en interne** qu'il faut encadrer
- ✓ La nature de ces données personnelles peut être **« sensible »** ce qui implique une vigilance accrue

- ► Impact de la dématérialisation des démarches administratives :

- ✓ **Concerne particulièrement les personnes en situation de précarité sociale** (accès aux prestations sociales/familiales, à un emploi, renouvellement des pièces d'identité, demandes de titre de séjour, demandes de logement social, etc.)
- ✓ **Conduit à de nombreux échanges** avec les organismes et les administrations, qui soulèvent de multiples enjeux en matière de protection des données comme la sécurité des échanges et la confidentialité des données (ex: échange de données OFII/SIAO, demandes de communication de données par divers services de l'Etat)

⇒ **Compte tenu de ces enjeux spécifiques au secteur social, la CNIL a adopté le 11 mars 2021 le Référentiel Social** (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)

PARTIE 2 – LE REFERENTIEL « SOCIAL » (GENERALITES)

1. ENJEUX SOULEVÉS DANS LE SECTEUR SOCIAL
2. QUE RECOUVRE LE RÉFÉRENTIEL SOCIAL?

La Fédération est co-financée par l'Union européenne

QUE RECOUVRE LE RÉFÉRENTIEL SOCIAL? (1/3)

► Pourquoi ce référentiel a été mis en place ?

✓ Cet outil vise à faciliter l'accompagnement des acteurs du secteur social et médico-social dans leur mise en conformité en matière de protection des données

► A qui s'adresse le Référentiel ?

✓ Il s'adresse aux acteurs du secteur social et médico-social notamment aux structures accompagnant des publics en situation de précarité sociale, des personnes en situation de handicap ou des personnes âgées

✓ S'agissant du secteur de l'inclusion sociale, une multitude d'acteurs sont visés notamment :

- Structures de l'IAE (Ateliers et chantiers d'insertion, entreprises d'insertion …..)
- Structures de l'AHI (SIAO, accueil de jour, CHRS, foyers de jeunes travailleurs, pensions de famille…)
- Structures du DNA (HUDA, CADA,CPH)
- Établissements médico-sociaux (appartement de coordination thérapeutique, lits halte soins santé, lits d'accueil médicalisés)
- Structures accueillant des personnes sous main de justice
- Structures accueillant des personnes victimes de violence
- Centres communaux d'action sociale (CCAS)

QUE RECOUVRE LE RÉFÉRENTIEL SOCIAL? (2/3)

► Quels traitements de données personnelles recouvrent le Référentiel ?

Traitements de données personnelles des personnes en difficulté accueillies/ accompagnées mis en œuvre par la structure (en tant que responsable de traitement)

Traitements de données personnelles mis en place dans le cadre de la gestion interne des structures
=> D'autres référentiels sont applicables (ex: RH)

Traitements de données personnelles mis en œuvre dans le cadre de l'accompagnement social fournis aux personnes en difficultés (en tant que sous-traitant)
Ex: SIAO et gestionnaires utilisant le SI SIAO

Les traitements de données mis en œuvre dans le cadre de la protection de l'enfance ont vocation a être régis par un référentiel spécifique dédié

► Que désignent « les personnes en difficultés » dont les données sont traitées ?

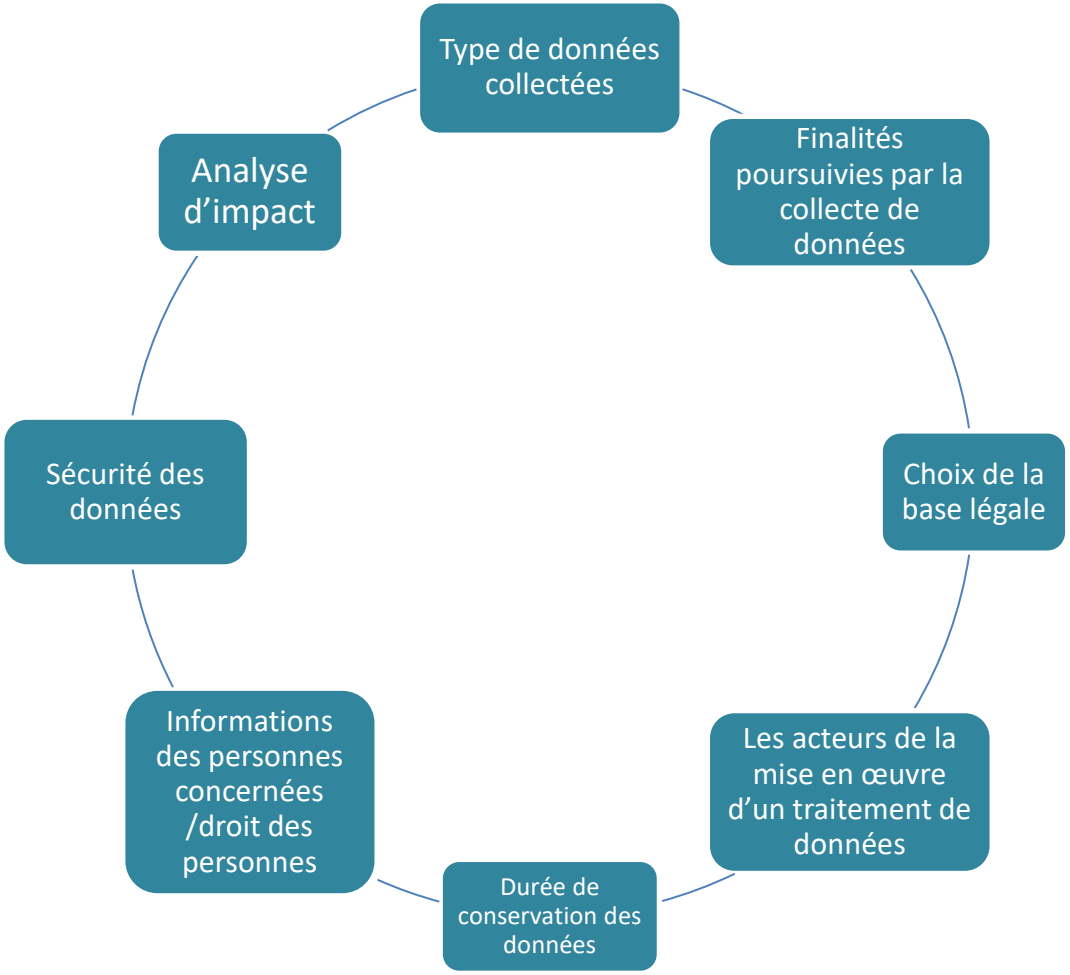
Le Référentiel en donne une définition et des illustrations y afférentes. Cette expression désignent celles qui *« sont menacées d'exclusion pour des motifs divers et confrontées à des problèmes eux-mêmes diversifiés »* telles que les demandeurs d'asile, les personnes en situation de grande précarité face au logement, à l'emploi, à l'accès aux soins, les personnes détenues/sortant d'établissement pénitentiaire…

⇒ Cette liste n'est pas exhaustive et peut englober d'autres types de publics faisant l'objet d'une exclusion sociale

QUE RECOUVRE LE RÉFÉRENTIEL SOCIAL? (3/3)

► Quels sont les points abordés par le Référentiel ?

Le Référentiel apporte des précisions sur l'application des règles en matière de protection des données dans le secteur social sur les points ci-dessous:



PARTIE 3 – LES PRINCIPAUX APPORTS DU REFERENTIEL « SOCIAL »

1. LES RELATIONS ENTRE CHAQUE ACTEUR
2. LE CHOIX DE LA BASE LÉGALE D'UN TRAITEMENT DE DONNÉES PERSONNELLES
3. LA DÉTERMINATION DE LA FINALITÉ D'UN TRAITEMENT DE DONNÉES PERSONNELLES
4. LE CHOIX DE LA DURÉE DE CONSERVATION DES DONNÉES
5. LES DROITS DES PERSONNES ACCOMPAGNÉES
6. LA SECURISATION DES DONNEES PERSONNELLES

La Fédération est co-financée par l'Union européenne

LES RELATIONS ENTRE CHAQUE ACTEUR : PANORAMA (1/5)

Définitions

Personnes concernées : Personnes physiques dont les données personnelles sont collectées

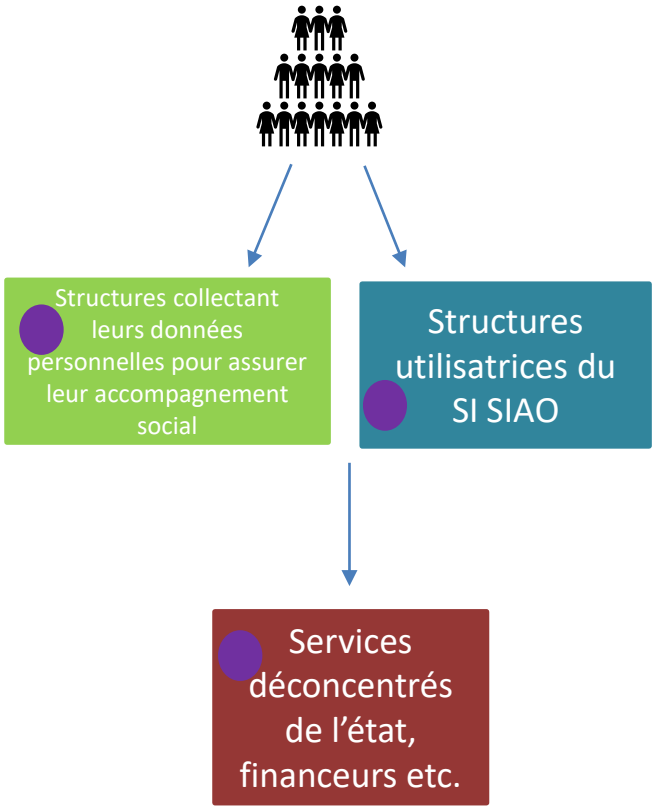
Responsable de traitements (RT) : entité qui détermine les objectifs et les modalités de collecte des données

Sous-traitant : entité qui collecte des données dans le cadre des missions confiées par le responsable de traitements

Destinataires: entité qui reçoit la communication des données personnelles ; certains pouvant être des tiers autorisés (entité publique habilitée par un texte à obtenir des données)

Délégué à la protection des données (DPO): conseille et accompagne le responsable de traitements dans sa mise en conformité

Illustrations des relations entre les acteurs



Un organisme peut être RT pour certaines activités *(ex: une association qui collecte des données personnelles dans le cadre de l'accompagnement social des personnes accompagnées)* et, simultanément, **sous-traitant pour d'autres activités** (ex : structures utilisatrices du SI-SIAO) et **destinataire de données personnelles** *(ex: communication de données par des professionnels de santé participant à l'accompagnement des personnes dans le respect des règles régissant le secret professionnel)*

Caractéristiques/attributions principales prévues par le RGPD

Personne concernées: disposent de droits qu'elles peuvent faire valoir auprès du responsable de traitements et de la CNIL

Le responsable de traitements doit assurer la conformité des traitements et informer les personnes des modalités de traitements des données et de leurs droits

Le sous-traitant agit sur les strictes instructions données par le RT

Les Tiers autorisés doivent justifier leur demande de communication de données

DPO : nomination non obligatoire dans le secteur mais fortement conseillée

LES RELATIONS ENTRE CHAQUE ACTEUR : ZOOM SUR LE RESPONSABLE DE TRAITEMENTS (2/5)

Le responsable de traitements (RT) …

- RT = La structure en tant que personne morale (ex : CADA, CHRS, ACI)

=> En cas de violation du RGPD par ses membres (salariés, bénévoles, stagiaires, etc), **c'est la personne morale qui sera sanctionnée et non ses dirigeants à titre personnel**

traite les données personnelles des publics pour des finalités légitimes et déterminées…

- Ex: collecte des données personnelles des publics accompagnés aux fins de gestion administrative de leur accueil (conclusion et suivi du contrat de séjour/conclusion et suivi du contrat de travail d'insertion), pour assurer leur accompagnement social

et doit assumer plusieurs obligations prévues par le RGPD

- Informer les personnes concernées
- Assurer la sécurité des données
- De tenir un registre de traitement des données
- De réaliser une analyse d'impact sur la protection des données (AIPD)

=> Pour en savoir plus, cliquez ici

Comment limiter les risques de violation du RGPD?

Juridique: prévoir une clause de confidentialité dans le contrat de travail et/ou une clause qui rappelle les obligations découlant du secret professionnel (lorsque les salariés y sont assujettis)

Pratique: former ses équipes notamment concernant le respect de la confidentialité et la sécurité des données des personnes accompagnées

LES RELATIONS ENTRE CHAQUE ACTEUR : ZOOM SUR LE SOUS-TRAITANT (3/5)

Sous-traitant

+ doit tenir en interne un registre de traitements pour ses activités de sous-traitance

Conclusion d'un contrat de sous-traitance qui prévoit obligatoirement plusieurs engagements:

- obligation de transparence et de traçabilité (ex: recenser par écrit les instructions du RT..) ;
- la prise en compte des principes de protection des données dès la conception des traitements;
- obligation de garantir la sécurité des données traitées ;
- obligation d'assistance, d'alerte et de conseil (informer le RT en cas de violation de données)

Modèle de clause de sous-traitance dans le Guide du sous-traitant de la CNIL

Responsable de traitements

LES RELATIONS ENTRE CHAQUE ACTEUR : ZOOM SUR LE DPO (4/5)

Missions du Délégué à la protection des données (DPO)

- Informer et conseiller le RT sur les sujets relatifs à la protection des données
- Contrôler le respect du RGPD et du droit national en matière de protection des données
- Conseiller le RT sur la réalisation d'une AIPD et d'en vérifier l'exécution
- Coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci (ex: faciliter l'accès aux données à la CNIL en cas de contrôle)

Prérequis pour les mener: indépendance du DPO

- **RT doit fournir les moyens nécessaires pour accomplir ses missions** (accès aux données, matériel adéquat…)
- **Ne doit pas** recevoir d'instructions sur la façon de traiter une affaire et ne doit pas être enjoint d'adopter un certain point de vue sur une question liée à la législation en matière de protection des données, par exemple, une interprétation particulière du droit
- **Prévention des conflits d'intérêts:** le DPO ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitements

Exercer une fonction de direction est par définition incompatible avec celle de DPO

NB: cela vaut aussi pour les DPO externes *(ex : DPO externe qui représenterait l'organisme devant une juridiction pour une affaire liée à la protection des données)*

Bonnes pratiques

❖ Pour éviter les conflits d'intérêts :

- recenser les fonctions qui seraient incompatibles avec celles de DPO;
- établir des règles internes sur ce sujet ;
- inclure une explication plus générale concernant les conflits d'intérêts;
- prévoir des garanties dans le règlement intérieur de l'organisme.

❖ Pour mutualiser les ressources

Recours à un DPO externe accompagnant plusieurs structures, dont les compétences sont certifiées par un des organismes agréés par la CNIL

Pour en savoir plus, consultez les lignes directrices relatives au DPO du CEPD

LES RELATIONS ENTRE CHAQUE ACTEUR : ZOOM SUR LE TIERS AUTORISE ET LE DESTINATAIRE (5/5)

- Les destinataires correspondent à une catégorie d'acteurs qui sont susceptibles de recevoir la communication de données personnelles

- Les tiers autorisés (autorités et organismes publics) constituent une catégorie spécifique de destinataires car la communication de données personnelles à ces derniers doit être prévue et encadrée précisément par le droit national ou européen.

Ex: l'administration fiscale est fondée à demander des informations sur des salariés afin de pratiquer des saisies sur salaires conformément au cadre légal de l'article L82 B du livre des procédures fiscales)

Point de vigilance:
Le RT doit garantir la sécurité des données (incluant leur confidentialité) et doit s'assurer de la légalité des demandes de communication de tiers.

- Que faire en cas de demande de communication de données d'un tiers ?

Il faut demander au tiers à l'origine de la demande (si les éléments suivants n'y figurent pas):
Quelle est la base juridique autorisant la demande de communication des données ?
Quelle est la finalité de la transmission des données demandées ?
Quelles sont précisément les données personnelles dont vous souhaitez la communication (afin de s'assurer qu'elles sont en adéquation avec la finalité de la transmission) ?
Quelles sont les mesures de sécurité mise en place pour l'envoi de ces données et leur traitement ?

En l'absence de retour satisfaisant, le RT est en droit de ne pas transmettre les données personnelles demandées

NB: modèle de réponse rédigé à une demande de communication non justifiée figurant en annexe du présent document

Pour aller plus loin: *guide du tiers autorisé* et *recueil des procédures – tiers autorisés*

PARTIE 3 – LES PRINCIPAUX APPORTS DU REFERENTIEL « SOCIAL »

1. LES RELATIONS ENTRE CHAQUE ACTEUR
2. LE CHOIX DE LA BASE LÉGALE D'UN TRAITEMENT DE DONNÉES PERSONNELLES
3. LA DÉTERMINATION DE LA FINALITÉ D'UN TRAITEMENT DE DONNÉES PERSONNELLES
4. LE TYPE DE DONNEES PERSONNELLES COLLECTABLES
5. LE CHOIX DE LA DURÉE DE CONSERVATION DES DONNÉES
6. INFORMATION ET DROITS DES PERSONNES ACCOMPAGNÉES
7. LA SECURISATION DES DONNEES PERSONNELLES

La Fédération est co-financée par l'Union européenne

LE CHOIX DE LA BASE LEGALE : DEFINITION (1/3)

► La base légale ou la base juridique d'un traitement est le fondement juridique qui autorise légalement sa mise en œuvre

Bases légales prévues par le RGPD	Précisions	Exemples de finalités associées par le Référentiel social
Consentement	Doit être recueilli valablement: libre, éclairé, spécifique, univoque)	Peu recommandé par le Référentiel social (cf slide suivant)
Contrat	Doit être nécessaire à l'exécution d'un contrat auquel la personne concernée et le RT sont parties	Fourniture de prestations définies par le contrat conclu entre la personne concernée et la structure de droit privée (ex: contrat de séjour conclu en CHRS, CADA; CDDI en structure de l'IAE …) *A noter: se référer au référentiel de la CNIL sur les RH pour les traitements de données personnelles se rattachant à la gestion des ressources humaines concernant les salariés en insertion au sein de SIAE (gestion du temps de travail, gestion de la formation etc.)*
Obligation légale	Doit imposer au RT une obligation impérative (issue du droit national ou du droit européen) de traiter des données personnelles et définir, au moins, les finalités du traitement concernées	Remontée des informations préalablement anonymisées à l'ARS, au Préfet et au Président du Conseil départemental concernant des dysfonctionnements graves ou évènements ayant pour effet de menacer ou de compromettre la santé, la sécurité ou le bien-être des personnes prises en charge (cf. arrêté du 28 décembre 2016 (NOR : AFSA1611822A))
Intérêts légitimes	Doit permettre d'accomplir les intérêts légitimes du RT sans pour autant créer un déséquilibre concernant les droits et intérêts des personnes concernées	Accompagnement social et médico-social des personnes concernées
Sauvegarde des intérêts vitaux	Se rapportent à des questions de vie, de mort ou de menaces relatives à une personne incapable de donner son consentement	Aucune finalité associée par le Référentiel social
Mission d'intérêt public	Doit être prévue par le droit européen ou le droit national	Instruction, gestion et, le cas échéant, ouverture des droits et/ou versement des demandes de prestations sociales légales

Bon à savoir : *plusieurs bases légales peuvent être valables pour fonder un seul et même traitement mais il faut en retenir seulement une : il reviendra au RT de choisir celle qui semble la plus appropriée*

LE CHOIX DE LA BASE LEGALE : ZOOM SUR LE CONSENTEMENT (2/3)

- Le consentement comme base légale est soumis à des règles strictes encadrant son recueil (n'imposant pas pour autant de formalisme particulier)

Dans le cadre de l'accompagnement social/médico-social des personnes, le recours au consentement est **déconseillé** par le Référentiel social estimant que **la vulnérabilité de ce public et l'altération du discernement en découlant peut rendre le consentement non valable**

- Spécificités pour les personnes en incapacité juridique

Pour les personnes en incapacité juridique (comme les majeurs sous mesure de protection juridique (tutelle, curatelle…) ou les mineurs non accompagnés), il convient de recueillir le consentement des représentants légaux si cette base légale est choisie.

En l'absence de représentant légal nommé : recourir à une autre base légale

Cliquez ici pour aller plus loin sur cette notion

Points de vigilance à observer quand la base légale du traitement choisie est le consentement

- Recueillir le consentement pour chaque finalité de traitement ;
- Pouvoir assurer la possibilité que la personne concernée puisse retirer son consentement à tout moment ;
- Informer la personne des modalités du traitement de ses données et de ses droits avant le recueil du consentement ;
- Faire en sorte que le choix de la personne soit exprimé de manière positive (ex: case à cocher);
- Garder une preuve de recueil du consentement (préférer un recueil écrit plutôt qu'à l'oral).

LE CHOIX DE LA BASE LEGALE : ZOOM SUR LES INTERETS LEGITIMES (3/3)

- Les intérêts légitimes du RT est une base légale qui est préconisée par le Référentiel social pour certaines finalités de traitements comme l'accompagnement social et médico-social des publics en situation de précarité.

- S'agissant de l'accompagnement social et médico-social des personnes, la collecte de données de santé se révèle nécessaire pour accomplir cette finalité de traitement. Or, la collecte de telles données, relevant de la catégorie des données sensibles, est par principe interdite par le RGPD à son article 9.

⇒ *Quelle solution mettre en place pour collecter valablement les données sensibles des personnes accompagnées strictement nécessaires à assurer leur accompagnement social et médico-social (accompagnement vers les soins par ex) ?*

L'article 9 précité prévoit des exceptions à cette interdiction. Le Référentiel social, reprenant les règles du RGPD, considère que la collecte de données sensibles (de santé) aux fins d'accompagnement est possible seulement si le consentement de la personne concernée est valablement recueilli dans les conditions du recueil du consentement).

PARTIE 3 – LES PRINCIPAUX APPORTS DU REFERENTIEL « SOCIAL »

1. LES RELATIONS ENTRE CHAQUE ACTEUR
2. LE CHOIX DE LA BASE LÉGALE D'UN TRAITEMENT DE DONNÉES PERSONNELLES
3. LA DÉTERMINATION DE LA FINALITÉ D'UN TRAITEMENT DE DONNÉES PERSONNELLES
4. LES CATEGORIES DE DONNEES PERSONNELLES
5. LE CHOIX DE LA DURÉE DE CONSERVATION DES DONNÉES
6. INFORMATION ET DROITS DES PERSONNES ACCOMPAGNÉES
7. LA SECURISATION DES DONNEES PERSONNELLES

La Fédération est co-financée par l'Union européenne

LA DÉTERMINATION DE LA FINALITÉ D'UN TRAITEMENT DE DONNÉES PERSONNELLES

Qu'est ce qu'une finalité?

- C'est l'objectif principal pour mettre un traitement de données personnelles en place devant poursuivre un but déterminé et légitime
  ⇒ Une fois la finalité déterminée, les données **ne pourront pas être traitées pour une autre finalité qui serait incompatible avec l'objectif initial**

- Chaque finalité doit **reposer sur une base juridique** et peut **regrouper plusieurs opérations de traitements**

Transmettre des données personnelles de personnes accompagnées collectées pour assurer leur accompagnement social à un tiers (chercheur par exemple) pour une autre finalité comme réaliser une étude à partir de ces données

Regrouper sous la finalité « gestion administrative des personnes accompagnées » les opérations de traitements de données personnelles suivantes:
- *la conclusion d'un contrat entre chaque personne accompagnée et la structure,*
- *le suivi du nombre de personnes accompagnées (formalisée par un tableau de suivi par exemple)*

Quelle est sa fonction?

- **Fonction décisive:** c'est au regard de la finalité du traitement que **la pertinence des données collectées va être évaluée et que leur durée de conservation va être fixée** (les données devant être conservées la durée nécessaire à l'accomplissement de la finalité *cf. slides sur la durée de conservation du présent document*)

Que dit le Référentiel social?

- Le référentiel social liste les finalités de traitements les plus répandues dans le secteur comme **l'accompagnement social et médico-social** (assurer le suivi des personnes dans l'accès aux droits, orientation des publics vers des structures adaptées à leurs besoins etc.) ou **la gestion administrative de l'organisme** etc.

=> **La liste n'est pas exhaustive:** vous pouvez traiter des données personnelles pour d'autres finalités que celles prévues sous réserve de respecter les principes du RGPD

Pour aller plus loin sur cette notion: https://www.cnil.fr/fr/definir-une-finalite

PARTIE 3 – LES PRINCIPAUX APPORTS DU REFERENTIEL « SOCIAL »

1. LES RELATIONS ENTRE CHAQUE ACTEUR
2. LE CHOIX DE LA BASE LÉGALE D'UN TRAITEMENT DE DONNÉES PERSONNELLES
3. LA DÉTERMINATION DE LA FINALITÉ D'UN TRAITEMENT DE DONNÉES PERSONNELLES
4. LES CATEGORIES DE DONNEES PERSONNELLES
5. LE CHOIX DE LA DURÉE DE CONSERVATION DES DONNÉES
6. INFORMATION ET DROITS DES PERSONNES ACCOMPAGNÉES
7. LA SECURISATION DES DONNEES PERSONNELLES

La Fédération est co-financée par l'Union européenne

LES CATEGORIES DE DONNEES PERSONNELLES

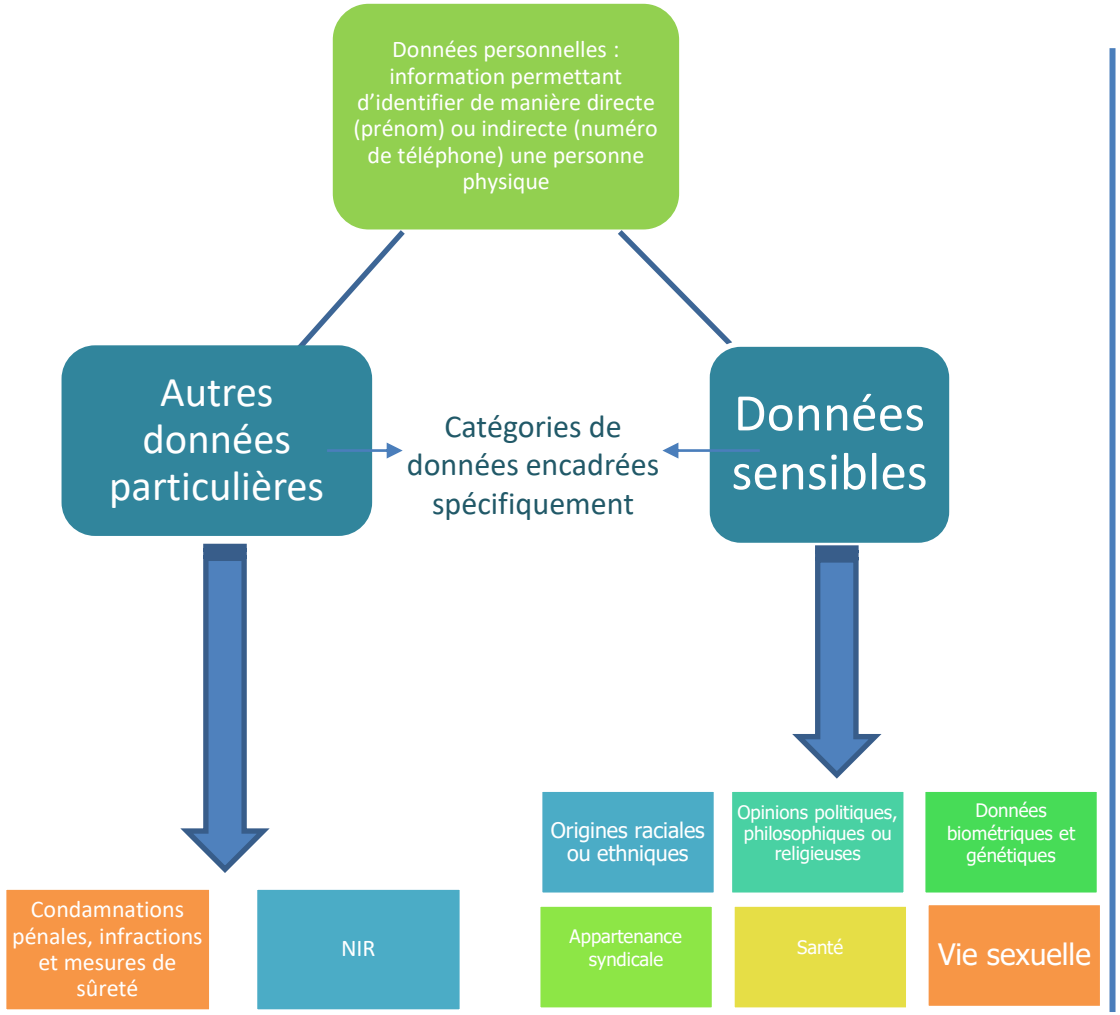
- Règle d'or pour tout type de données personnelles: respect du principe de minimisation des données

⇒ Collecte des données nécessaires à l'accomplissement de la finalité (prohibition de la collecte de données « au cas où »)

Numéro d'inscription des personnes (NIR):
Collecte autorisée uniquement dans les cas prévus par le décret n° 2019-341 du 19 avril 2019
pour plus d'information: FAQ CNIL dédiée

Collecte de données de condamnations et infractions pénales/mesure de sûreté possible que pour :

- les associations de défense de victimes agréées par le Ministère de la Justice
- les associations d'aide à la réinsertion des personnes placées sous-main de justice
- certains ESMS notamment ceux intervenant dans le domaine de la PJJ ou gérant des lieux d'accueil et de vie



Principe d'interdiction de collecte des données sensibles sauf en cas de :

- Recueil valable du consentement de la personne

ex: données de santé collectées nécessaires à l'accompagnement social des personnes (base légale: intérêts légitimes) tel que préconisé par le Référentiel social

- Nécessité en vue d'assurer une prise en charge sanitaire ou sociale en vertu du droit national ou européen

ex : données collectées pour assurer un accompagnement juridique des personnes demandeurs d'asile

Fédération des acteurs de la solidarité

PARTIE 3 – LES PRINCIPAUX APPORTS DU REFERENTIEL « SOCIAL »

1. LES RELATIONS ENTRE CHAQUE ACTEUR
2. LE CHOIX DE LA BASE LÉGALE D'UN TRAITEMENT DE DONNÉES PERSONNELLES
3. LA DÉTERMINATION DE LA FINALITÉ D'UN TRAITEMENT DE DONNÉES PERSONNELLES
4. LES CATEGORIES DE DONNEES PERSONNELLES
5. LE CHOIX DE LA DURÉE DE CONSERVATION DES DONNÉES
6. INFORMATION ET DROITS DES PERSONNES ACCOMPAGNÉES
7. LA SECURISATION DES DONNEES PERSONNELLES

La Fédération est co-financée par l'Union européenne

LE CHOIX DE LA DURÉE DE CONSERVATION DES DONNÉES : REGLES GENERALES (1/2)

► La règlementation sur la protection des données (en format papier et numérique) prévoit qu'elles doivent être conservées uniquement la durée nécessaire à l'accomplissement de la finalité

Période 1 - durée de conservation (base active)

- **Règles de détermination de la durée de conservation**
  - Vérifier si une durée prévue par les textes (loi ou textes règlementaires) s'applique
  À défaut: application de la durée de référence dans le secteur prévue par le Référentiel social (2 ans compter du dernier contact avec la personne accompagnée) ;
  Si cela ne convient pas, c'est au RT de déterminer une autre durée et d'être en mesure de le justifier (prohibition de la conservation de données personnelles « au cas où »)
- **Accès aux données autorisé uniquement aux personnes habilitées en interne**

Exemple : *conservation de CDDI ayant été prolongés jusqu'à 60 mois (durée maximale prévue à l'article L5132-15-1 du code du travail) accessibles qu'au personnel accompagnant la personne*

S'il n'y pas d'intérêt à archiver les données

Période 2 – Archivage

- Possibilité d'archiver une fois la durée de conservation en base active expirée
- Conservation en archivage uniquement s'il y a un intérêt réel
- Accès aux données uniquement aux personnes habilitées en interne

=> Les habilitations sont davantage restreintes comparées à la période 1 compte tenu de la « nouvelle finalité » justifiant l'archivage.

Exemple: *archivage des CDDI durant 5 ans en cas de conservation (durée de la prescription civile) accessibles qu'au personnel gérant le contentieux (le personnel accompagnant la personne n'ayant aucune raison d'y avoir accès)*

Période 3 – Suppression des données ou anonymisation

- Suppression des données doit se faire de manière sécurisée
- Anonymisation des données doit garantir l'absence de possibilité de réidentification des personnes

Exemple: *après l'archivage de 5 ans des CDDI, suppression des contrats en format papier en utilisant une broyeuse sans oublier ceux en format numérique*

Pour plus d'informations, consultez le guide pratique sur les durées de conservation de la CNIL

Votre structure peut être soumise à la règlementation sur les archives publiques (cf.Annexe 2)

Fédération des acteurs de la solidarité

LE CHOIX DE LA DURÉE DE CONSERVATION DES DONNÉES : FOCUS SUR LA DUREE DE CONSERVATION DE REFERENCE (2/2)

Conservation des données durant 2 ans

Durée de référence préconisée par le Référentiel social pour toutes les finalités (si un texte ne prévoit aucune durée de conservation)

Conserver les données « au cas où » les personnes reviendraient demander des documents administratifs pour assurer la continuité de leurs démarches administratives

Bonnes pratiques:

- Proposer aux personnes accompagnées de stocker leurs données sur un coffre fort numérique*
- Proposer de restituer le dossier de la personne accompagnée constitué de ses documents administratifs à cette dernière lorsqu'elle quitte la structure (droit à la portabilité des données)

=> Dans tous les cas, détruire les données personnelles des personnes accompagnées une fois la durée de conservation expirée

*C'est un outil qui permet de stocker dans un espace numérisé leurs documents administratifs et de donner un accès à ces données aux acteurs que la personne accompagnée aura choisie (comme la structure qui l'accompagne) qui peut être modifié à tout moment. Cela peut être une solution alternative intéressante pour que les personnes puissent avoir accès à leurs données.
Divers acteurs en mettent en place comme La Poste (avec son coffre-fort numérique Digiposte qui est gratuit) et l'association Reconnect.

Fédération des acteurs de la solidarité

PARTIE 3 – LES PRINCIPAUX APPORTS DU REFERENTIEL « SOCIAL »

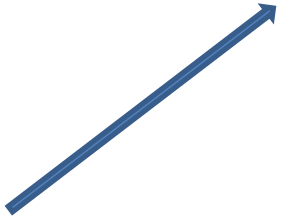
1. LES RELATIONS ENTRE CHAQUE ACTEUR
2. LE CHOIX DE LA BASE LÉGALE D'UN TRAITEMENT DE DONNÉES PERSONNELLES
3. LA DÉTERMINATION DE LA FINALITÉ D'UN TRAITEMENT DE DONNÉES PERSONNELLES
4. LES CATEGORIES DE DONNEES PERSONNELLES
5. LE CHOIX DE LA DURÉE DE CONSERVATION DES DONNÉES
6. INFORMATION ET DROITS DES PERSONNES ACCOMPAGNÉES
7. LA SECURISATION DES DONNEES PERSONNELLES

La Fédération est co-financée par l'Union européenne

INFORMATION ET DROITS DES PERSONNES ACCOMPAGNÉES

Éléments obligatoires à indiquer dans l'information destinée aux personnes

- Identité et coordonnées du responsable
- Finalités
- Caractère obligatoire ou facultatif des réponses pour les formulaires
- Conséquence du défaut de réponse
- Droit de réclamation auprès de la CNIL
- Destinataires des données
- Durée de conservation
- Coordonnées du DPO
- Base juridique du traitement
- Droits des usagers (portabilité, accès rectification, opposition etc.)



Caractéristique de l'information : concise, transparente, compréhensible et aisément accessible aux personnes

Délai d'information des personnes : **au moment de la collecte des données quand elle est directe** (1 mois au plus tard quand elle est indirecte)

Forme de l'information : **écrite** (méthode FALC à privilégier) dans tout document pertinent (livret d'accueil, contrat de séjour, contrat de travail pour l'IAE) et **orale** pour s'assurer de la bonne compréhension des personnes concernées

Type de droit	Définition
Accès	**permet de demander une copie des données pour en vérifier le contenu :** porte sur les données administratives les concernant et sur d'autres documents figurant dans leur dossier sous réserve du respect des droits des tiers et du secret (secret des correspondances, secret de l'enquête/ instruction pour les documents judiciaires …).
Rectification	**permet de demander la rectification de données personnelles**
Effacement (le cas échéant à la limitation des données collectées)	**permet de demander l'effacement des données personnelles,** par exemple une fois le retrait du consentement exercé ou à l'issue de l'expiration de la durée de conservation des données si cela n'a pas été déjà effectué (sauf si le traitement est fondé sur une obligation légale)
Retrait du consentement	**permet de retirer son consentement au traitement des données personnelles à tout moment**
Opposition	**permet de s'opposer au traitement de données personnelles par la structure** ; le référentiel précisant que pour les traitements relatifs à l'accompagnement social, la personne pourra s'y opposer **uniquement lorsque le traitement est mis en œuvre sur la base légale de l'intérêt légitime du responsable de traitement ou pour l'exécution d'une mission d'intérêt public**
Portabilité	**permet à la personne de récupérer ses données et/ou de demander leur transmission à une autre personne/organisme.** Ce droit existe uniquement pour les traitements de données automatisés fondés sur le consentement de la personne ou sur l'exécution d'un contrat, pas dans les autres cas.

FALC : Facile à lire et à comprendre

Cliquez ici pour aller plus loin et cliquez ici pour des exemples de mentions d'information

PARTIE 3 – LES PRINCIPAUX APPORTS DU REFERENTIEL « SOCIAL »

1. LES RELATIONS ENTRE CHAQUE ACTEUR
2. LE CHOIX DE LA BASE LÉGALE D'UN TRAITEMENT DE DONNÉES PERSONNELLES
3. LA DÉTERMINATION DE LA FINALITÉ D'UN TRAITEMENT DE DONNÉES PERSONNELLES
4. LES CATEGORIES DE DONNEES PERSONNELLES
5. LE CHOIX DE LA DURÉE DE CONSERVATION DES DONNÉES
6. INFORMATION ET DROITS DES PERSONNES ACCOMPAGNÉES
7. LA SECURISATION DES DONNEES PERSONNELLES

La Fédération est co-financée par l'Union européenne

LA SECURISATION DES DONNEES PERSONNELLES

- Chaque acteur doit assurer la sécurité des données personnelles en mettant en place des mesures adaptées visant à préserver la confidentialité, l'intégrité et la pérennité des données d'autant que des enjeux en matière de sécurité des données dans le secteur sont assez importants (cf. partie 1 du présent document).

- Le Référentiel social reprend les mesures de sécurité basiques comme le changement régulier de mots de passe, la mise en place d'une charte informatique, d'une politique de gestion des habilitations d'accès aux données et de traçabilité des accès, la mise en place de mots de passe sur les fichiers contenant des données personnelles envoyés par email etc. Ces mesures ne sont pas exhaustives et doivent être adaptées en fonction des risques rencontrés par chaque structure.

Pour plus d'informations, consultez le guide sur la protection des données de la CNIL.

- Il convient également de mettre en place des bonnes pratiques pour l'accompagnement des personnes accueillies dans leurs démarches administratives :
  - Veiller à effacer les traces après chaque démarche réalisée en ligne ;
  - En cas de réalisation des démarches à leur place : demander leur accord pour utiliser ses informations (modèle de mandat de la CNIL ou mandat oral si urgence + respect bonnes pratiques de la CNIL) ;
  - Outils utiles pour la gestion des mots de passe et pour la confidentialité des documents administratifs : France Connect / coffre fort numérique (Reconnect, La Poste, La clé solidaire …).

Pour aller plus loin: recommandations de la CNIL pour accompagner les usagers du secteur.

Fédération des acteurs de la solidarité

PARTIE 4 – LA DOCUMENTATION DE LA MISE EN CONFORMITE

1. RAPPEL SUR LES ETAPES DE LA DEMARCHE DE MISE EN CONFORMITE
2. LA MISE EN PLACE D'UN REGISTRE DE TRAITEMENTS DE DONNEES
3. L'ELABORATION D'UNE AIPD

La Fédération est co-financée par l'Union européenne

RAPPEL SUR LES ETAPES DE LA DEMARCHE DE MISE EN CONFORMITE (1/2)

1/ Recenser de façon précise les traitements de données personnelles existants dans la structure

⇒ L'utilisation du registre de traitements pour les recenser est conseillé afin de collecter l'ensemble des informations pertinentes pour pouvoir évaluer la conformité des traitements à la règlementation sur la protection des données

2/ Identifier et prioriser les actions à mener pour leur mise en conformité aux nouvelles obligations

3/ Identifier les risques associés aux opérations de traitement et prendre les mesures nécessaires à leur prévention ;

4/ Mettre en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment et de l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : conservation des données, faille de sécurité, gestion des demandes d'exercice des droits, gestion des demandes d'habilitation etc.)

Pour mener à bien l'ensemble de ces étapes, il est fortement conseillé d'établir une gouvernance en interne pour le pilotage de la mise en conformité (personne/ groupe de travail en charge du pilotage, désignation d'un DPO qui le/la conseillera), en cas de pluralité d'établissements, désignation d'un référent RGPD par établissement qui centralisera les sujets

RAPPEL SUR LES ETAPES DE LA DEMARCHE DE MISE EN CONFORMITE : DOCUMENTATION OBLIGATOIRE (2/2)

- Registre de traitements (pour les activités en qualité de ST et de RT)

- AIPD OBLIGATOIRE avant la mise en place d'un traitement de données pour le secteur car les traitements peuvent présenter des risques élevés pour la protection des données personnelles .

  La CNIL a fixé la liste des traitement où l'AIPD est obligatoire. Y figure:

✓ L' Instruction des demandes et gestion des logements sociaux

✓ Les traitements ayant pour finalité l'accompagnement social ou médico-social des personnes

NB: régulariser les AIPD non effectuées pour les traitements précités qui auraient déjà été mis en œuvre

- Information des personnes : mentions d'information, modèles de recueil du consentement des personnes concernées, procédures mises en place pour l'exercice des droits

PARTIE 4 – LA DOCUMENTATION DE LA MISE EN CONFORMITE

1. RAPPEL SUR LES ETAPES DE LA DEMARCHE DE MISE EN CONFORMITE
2. LA MISE EN PLACE DES REGISTRES DE TRAITEMENTS DE DONNEES
3. L'ELABORATION D'UNE AIPD

La Fédération est co-financée par l'Union européenne

LA MISE EN PLACE DES REGISTRES DE TRAITEMENTS DE DONNEES

Qu'est – ce qu'un registre de traitements ?

- Outil ayant pour objectif de recenser les traitements de données personnelles existants dans une structure participant ainsi à la documentation de la conformité
- Outil reflétant la réalité des traitements de données personnelles mis en œuvre et permettant d'avoir une vue d'ensemble de l'utilisation de ces dernières
- Complétude du registre de traitement = une étape essentielle pour déduire un plan d'action de mise en conformité des traitements de données ; la tenue d'un registre étant obligatoire (article 30 RGPD)

Deux types de registres de traitements prévus par le RGPD :

	Registre des activités de traitement du responsable de traitement (RT)	Registre des activités de traitement du sous-traitant (ST)
Éléments obligatoires	• Coordonnées du RT, du DPO (du RT conjoint s'il en existe), finalités, sous-finalités du traitements • Catégorie des personnes concernées, de données personnelles, de destinataires • Existence de transfert de données hors UE et le cas échéant les garanties prévues • Durées de conservation • Description générale des mesures de sécurité	• Coordonnées du RT, des ST ultérieurs éventuels • Catégories de traitements (opérations effectuées pour le compte du RT), • Transferts de données hors UE et, dans certains cas, les garanties prévues • Descriptions générales des mesures de sécurité
Exemples d'activités de traitement à faire figurer	Déclaration d'embauche des salariés en insertion, admission d'une personne au sein d'une structure (CHRS, accueil de jour, CADA ..)	Traitements réalisés dans le cadre de l'utilisation du SI SIAO par les SIAO et gestionnaires

PARTIE 4 – LA DOCUMENTATION DE LA MISE EN CONFORMITE

1. RAPPEL SUR LES ETAPES DE LA DEMARCHE DE MISE EN CONFORMITE
2. LA MISE EN PLACE DES REGISTRES DE TRAITEMENTS DE DONNEES
3. L'ELABORATION D'UNE AIPD

La Fédération est co-financée par l'Union européenne

L'ELABORATION D'UNE AIPD

Définition analyse d'impact sur la protection des données (AIPD)

- S'inscrit dans la démarche **responsabilisation globale prévue par le RGPD** *(accountability)*
- Permet de mesurer la conformité au RGPD d'un traitement de données et s'il respecte la vie privée des personnes concernées
- Outil obligatoire pour les traitements de données ayant pour finalité l'accompagnement social ou médico-social

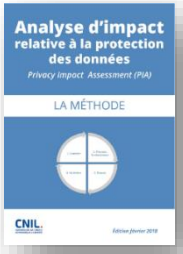
Contenu requis par le RGPD

- Description systématique des opérations de traitement envisagées et les finalités du traitement
- Evaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- Evaluation des risques sur les droits et libertés des personnes concernées et les mesures envisagées pour faire face aux risques

Bonnes pratiques pour mener une AIPD

- **Recenser les traitements de données** ayant pour finalité l'accompagnement social/médico-social des personnes
- **Réunir l'ensemble des acteurs pertinents en interne :** service informatique, travailleurs sociaux/bénévoles, direction, chefs de service pour avoir le maximum d'éléments pertinents à analyser
- **Désigner un.e pilote de cette AIPD** qui sera en charge de coordonner l'ensemble des acteurs pertinents en interne

- Outils de la CNIL pour accompagner les RT à construire leur AIPD : 3 guides, un exemple d'AIPD, un logiciel *PIA*



4 axes d'étude :
- *étude du contexte du traitement*
- *étude des mesures garantissant le respect de la vie privée des personnes*
- *études des risques liés à la sécurité des données*
- *validation de l'AIPD*

Modèles d'analyse pour les 4 axes d'étude cités dans le guide sur la méthode

Contient:
- les **définitions clés** pour mener un AIPD
- **l'échelle et les règles pour estimer la gravité d'un risque** d'atteinte à la vie privée
- un **catalogue de mesures de sécurité**

Exemple d'AIPD visant à illustrer les attentes minimales sans exploiter des bases de connaissances particulières

Logiciel « *PIA* » développé par la CNIL en accès libre destiné aux responsables de traitement pas ou peu familier avec la démarche de l'AIPD

Fédération des acteurs de la solidarité

ANNEXES

1. ANNEXE 1 : MODELE DE REPONSE A UNE DEMANDE DE COMMUNICATION DES DONNEES
2. ANNEXE 2 : ZOOM SUR LES ARCHIVES PUBLIQUES
3. ANNEXE 3 : LES LIENS UTILES VERS LES OUTILS DE LA CNIL

La Fédération est co-financée par l'Union européenne

ANNEXE 1: Modèle de réponse à une demande de communication d'un tiers

[Ce modèle est à adresser en cas de demande de communication d'un tiers ne présentant pas les justifications nécessaires que la CNIL impose]

Nous avons bien reçu votre demande visant à ce que nous vous transmettions des données à caractère personnel des personnes accueillies par notre structure. En tant que responsable du traitement des données et en application du RGPD, nous sommes contraints de vous demander des informations complémentaires avant toute transmission. Par conséquent, pourriez-vous nous préciser :

Quelle est la base juridique autorisant la demande de communication des données ?

Quelle est la finalité de la transmission des données demandées ?

Quelles sont précisément les données personnelles dont vous souhaitez la communication ?

Quelles sont les mesures de sécurité mises en place pour l'envoi de ces données et leur traitement ?

Nous restons à votre disposition pour toute question complémentaire,

ANNEXE 2 : Focus sur les archives publiques

- Certaines structures sont assujetties à la règlementation sur les archives publiques qui prévoit des règles spécifiques sur la durée de conservation des données revêtant un intérêt public.

- Le champ d'application des archives publiques est assez large:
  - Applicable aux structures publiques (CCAS, GIP) ou une structure privée exerçant une mission de service public ;
  - Applicable aux documents produits ou reçus par un organisme public ou un organisme privé chargé de mission de service public.

⇒ En cas de difficultés à déterminer si votre structure relève de cette règlementation, n'hésitez pas à vous adresser à la CNIL ou au service d'archives publiques territorialement compétent en consultant l'annuaire France Archives.

- Les conséquences principales de l'application de cette règlementation sont les suivantes :
  - **Les durées de conservation sont plus longues et déterminées en fonction de la durée d'utilité administrative des données (DUA)** fixées par des instructions du Service Interministériel des Archives de France (SIAF) ou, à défaut, par le service d'archives territorialement compétent ;

  - **le sort final des données sera tranché**, à l'issue de l'expiration de la DUA , soit via **les instructions nationales** si elles sont applicables ou par **le service d'archives territorialement compétent** (destruction ou conservation des données par exemple).

Fédération des acteurs de la solidarité

ANNEXE 3: Les liens utiles vers les outils de la CNIL (1/2)

- UNE FORMATION POUR TOUS
  - MOOC l'atelier RGPD
- OUTILS GENERAUX DE MISE EN CONFORMITE
  - **Démarche de la mise en conformité**
    - Un guide pratique de sensibilisation au RGPD (qui vaut aussi pour les associations)
    - 4 étapes pour commencer sa mise en conformité
    - 6 étapes pour aller plus loin
  - **Analyse d'impact sur la protection des données**
    - Outils (guides et logiciel PIA) mis en place par la CNIL pour réaliser une AIPD
    - Liste des traitements avec AIPD obligatoire
  - **Modèles (registre de traitements / mention d'information)**
    - Registre de traitements (responsable de traitement)
    - Exemple de mention d'informations
  - **Relations avec les tiers :**
    - Guide du sous-traitant
    - Guide des tiers autorisés
- SERVICES EN LIGNE
  - Désignation du DPO
  - Envoyer son analyse d'impact à la CNIL
  - Notifier une violation de données

ANNEXE 3: Les liens utiles vers les outils de la CNIL (2/2)

➢ OUTILS DU SECTEUR SOCIAL ET MEDICO-SOCIAL

- Outils généraux
  - Référentiel pour le secteur social et médico-social
  - La FAQ relative au Référentiel pour le secteur social et médico-social
  - Les grandes notions dans le secteur social
  - Décret cadre NIR (numéro de sécurité sociale) dans le secteur social
- Outils relatifs à la protection des données des personnes accompagnées
  - Kit d'information pour les travailleurs sociaux
  - Protéger les données de vos usagers
  - 12 conseils pour utiliser un ordinateur public en toute sécurité
  - Quiz « les Incollables » sur la protection des données à destination des jeunes