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

Adopté le 11 mars 2021

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. À qui s'adresse ce référentiel ?

Ce référentiel s'adresse aux **organismes privés ou publics, quelle que soit leur forme juridique,** ci-après « les **organismes** »**, qui accueillent, hébergent ou accompagnent sur le plan social et/ou médico-social les personnes âgées, les personnes en situation de handicap et celles en difficulté.**

Le présent référentiel est susceptible d'intéresser les organismes suivants **(liste non exhaustive)** :

- les conseils départementaux ;
- les centres communaux d'action sociale (CCAS) ;
- les établissements d'hébergement pour les personnes âgées dépendantes (EHPAD) ;
- les maisons départementales pour les personnes handicapées (MDPH) ;
- les services d'aide à l'accompagnement à domicile (SAAD) ;
- les services de soins infirmiers à domicile (SSIAD) ;
- les services d'accompagnement médico-social pour adultes handicapés (SAMSAH) ;
- les services d'éducation spéciale et de soins à domicile (SESSAD) ;
- les centres médico-psycho-pédagogiques (CMPP) ;
- les centres d'action médico-sociale précoce (CAMSP) ;
- les établissements et service d'aide par le travail (ESAT) ;
- les maisons d'accueil spécialisées (MAS) ;
- les instituts médico-éducatifs (IME) ;
- les instituts thérapeutiques, éducatifs et pédagogiques (ITEP) ;
- les services d'accompagnement à la vie sociale (SAVS) ;
- les services d'insertion par l'activité économique (SIAE) ;
- les pôles de compétences et de prestations externalisées (PCPE) ;
- les plateformes de coordination et d'orientation (PCO) ;
- les accueillants familiaux accueillant à titre onéreux des personnes âgées ou en situation de handicap ;
- les organismes chargés de la gestion d'un régime de base de la sécurité sociale légalement obligatoire ou du service des allocations, prestations et aides mentionnés dans le code de la sécurité sociale ou du code de l'action sociale et des familles ;
- les associations de droit privé créées sous la loi de 1901 ayant pour mission l'accueil, l'hébergement, l'accompagnement et le suivi social et médico-social des personnes âgées, des personnes en situation de handicap et de celles en difficulté ;
- les établissements sociaux et médico-sociaux listés par les dispositions de l'article L. 312-1 du code de l'action sociale et des familles (CASF).

Dans ce contexte, ces organismes sont amenés à mettre en œuvre des traitements automatisés en tout ou en partie, ainsi que des traitements non automatisés de données à caractère personnel, en tant que responsable de traitement, ce qui les soumet au respect des règles relatives à la protection des données.

Les organismes mettant en œuvre des traitements dans ce cadre doivent s'assurer de leur conformité :

- aux dispositions du règlement général sur la protection des données (RGPD) ainsi qu'à celles de la loi du 6 janvier 1978 modifiée (loi « informatique et libertés », ou LIL) ;
- aux autres règles éventuellement applicables, conformément à la réglementation en vigueur, notamment le CASF et le code de la santé publique (CSP).

Sont exclus du champ d'application du référentiel en raison de leurs spécificités, les traitements mis en œuvre par :

- les organismes de droit privé et/ou public dans le cadre de la prévention et la protection de l'enfance ;
- les mandataires judiciaires à la protection des majeurs.

2. Portée du référentiel

Ce référentiel porte sur les traitements de données à caractère personnel mis en œuvre couramment par les organismes dans le cadre de l'accompagnement social et/ou médico-social qu'ils fournissent aux personnes âgées, en situation de handicap ou en difficulté (les personnes 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, les demandeurs d'emploi, les personnes en difficulté financière, etc.).

Il a pour objectif de fournir aux organismes mettant en œuvre de tels traitements un outil d'aide à la mise en conformité à la réglementation relative à la protection des données à caractère personnel.

Les traitements mis en œuvre par les organismes dans le cadre de l'accompagnement social et/ou médico-social doivent être inscrits dans le registre prévu à l'article 30 du RGPD (voir modèle de registre).

Ce référentiel n'a pas de valeur contraignante. Il permet en principe d'assurer la conformité des traitements de données mis en œuvre par les organismes aux principes relatifs à la protection des données, dans un contexte d'évolution des pratiques à l'ère du numérique.

Les organismes qui s'écarteraient du référentiel au regard des conditions particulières tenant à leur situation peuvent le faire.

Il peut néanmoins leur être demandé de justifier de l'existence d'un tel besoin et des mesures mises en œuvre afin de garantir la conformité des traitements à la réglementation en matière de protection des données à caractère personnel.

Le référentiel n'a pas pour objet d'interpréter les règles de droit autres que celles relatives à la protection des données à caractère personnel. Il appartient aux acteurs concernés de s'assurer qu'ils respectent les autres réglementations qui peuvent par ailleurs trouver à s'appliquer (p. ex. : CASF, CSP, *etc.*).

Ce référentiel constitue également une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD), dans le cas où celle-ci est nécessaire.

Les organismes peuvent également se reporter aux outils méthodologiques proposés par la CNIL sur son site web en vue de faciliter la mise en conformité des traitements mis en œuvre. Ils seront ainsi à même de définir les mesures permettant d'assurer la nécessité et la proportionnalité de leurs traitements (points 3 à 7), de garantir les droits des personnes (points 8 et 9) et la maîtrise de leurs risques (point 10). L'organisme pourra également s'appuyer sur les lignes directrices de la CNIL sur les AIPD. Si l'organisme en a désigné un, le délégué à la protection des données (DPD/DPO) devra être consulté.

3. Objectif(s) poursuivi(s) par le(s) traitement(s) (Finalités)

Les traitements mis en œuvre doivent répondre à un objectif précis et être justifiés au regard des missions et des activités des organismes.

Les traitements relatifs à l'accueil, l'hébergement et l'accompagnement social et médico-social des personnes peuvent notamment être mis en œuvre afin :

a) **de fournir les prestations** définies dans le cadre d'un contrat conclu entre l'organisme et la personne concernée ou son représentant légal et, le cas échéant, **d'assurer la gestion du dossier administratif de la personnes concernée** (gestion des rendez-vous médicaux et/ou sociaux, gestion des visites familiales, le cas échéant, etc.) ;

Exemples pour les personnes en situation de handicap ou les personnes âgées (liste non exhaustive) :

- le contrat de séjour ou le document individuel de prise en charge (DIPEC) prévu par l'article L. 311-4 du CASF entre l'organisme (EHPAD, les foyers d'hébergement pour adultes handicapés, etc.) et la personne concernée ou son représentant légal ;
- le contrat d'accueil à domicile entre l'accueillant familial et la personne accueillie ou son représentant légal ;
- le contrat de soutien et d'aide par le travail entre l'établissement ou le service d'aide par le travail et chaque travailleur en situation de handicap.

Exemples pour les personnes en difficulté (liste non exhaustive) :

- le contrat d'engagement réciproque (CER) ou le projet personnalisé d'accès à l'emploi (PPAE) conclu entre le bénéficiaire du revenu de solidarité active (RSA) et le président du conseil départemental pour améliorer l'insertion professionnelle ;
- le contrat d'hébergement conclu entre le bénéficiaire et l'organisme assurant l'accueil des personnes en situation d'urgence.

b) d'instruire, de gérer et, le cas échéant, d'ouvrir les droits et/ou verser les prestations sociales légales et facultatives ;

Exemples d'aides légales pour les personnes en situation de handicap ou les personnes âgées (liste non exhaustive) :

- l'aide sociale à l'hébergement (ASH) ;
- l'allocation personnalisée d'autonomie (APA) ;
- l'allocation aux adultes handicapées (AAH) ;
- l'allocation d'éducation de l'enfant handicapé (AEEH) ;
- la prestation de compensation du handicap (PCH) ;
- la carte mobilité inclusion (CMI).

Exemples d'aides légales pour les personnes en difficulté (liste non exhaustive) :

- le revenu de solidarité active (RSA) ;
- l'allocation de logement sociale (ALS).

Exemples d'aides facultatives (liste non exhaustive) :

- les aides ménagères ;
- les aides au transport ;
- la prise en charge des frais d'obsèques ;
- le règlement des factures de gaz et/ou d'électricité ;
- le fond d'aide aux jeunes.

c) d'offrir un accompagnement social et médico-social adapté aux difficultés rencontrées ayant notamment pour objet **d'élaborer un projet personnalisé d'accompagnement** au regard des habitudes de vie, des demandes particulières, des besoins particuliers, de l'autonomie physique et psychique de la personne et d'en assurer le suivi conformément aux dispositions des articles L. 311-3 du CASF, **d'assurer le suivi des personnes dans l'accès aux droits** notamment l'assistance dans les relations et les

démarches à effectuer et, le cas échéant, **d'orienter les personnes vers les structures compétentes susceptibles de les prendre en charge** ;

Exemples pour les personnes en situation de handicap ou les personnes âgées (liste non exhaustive) :

- assurer un suivi médicalisé adapté à l'état de la personne ;
- accompagner les personnes dans les actes essentiels de leur vie quotidienne (p. ex. : aide à la préparation des repas, aide au ménage et à l'entretien du domicile, aide aux déplacements, aide à la toilette, etc.) ;
- assurer la gestion des dossiers individuels de soins dans le cadre du suivi médical des personnes comprenant la gestion des remboursements des frais médicaux ;
- assurer la gestion des demandes de places en établissement ou service, médicalisé ou non ;
- assurer l'organisation et le suivi des parcours d'insertion et/ou d'intégration scolaire, sociale et professionnelle ;
- élaborer un registre communal d'alerte et d'information des populations ;
- assurer l'accès aux droits relatifs à la fin de vie (information quant à la possibilité de vivre ses derniers jours accompagné et apaisé, accompagnement dans la rédaction des « directives anticipées », etc.) ;
- assurer l'assistance dans le cadre des démarches administratives numériques à effectuer auprès des plus fragiles et notamment les personnes qui ne sont pas en capacité de se déplacer (un guide de bonnes pratiques à destination des professionnels est disponible sur le site web de la CNIL).

Exemples pour les personnes en difficulté (liste non exhaustive) :

- assurer l'organisation et le suivi des parcours d'insertion/de réinsertion et/ou d'intégration scolaire, sociale et professionnelle ;
- assurer l'accompagnement et le suivi éducatif et budgétaire des personnes et prévenir le surendettement ;
- assurer la gestion des demandes d'hébergement et d'accès au logement ;
- assurer la gestion des impayés et prévenir les expulsions locatives ;
- assurer le suivi des personnes et des familles reçues dans le cadre de la médiation familiale, sociale ou pénale, à l'exclusion des mesures relevant de l'aide sociale à l'enfance ;
- assurer le suivi de l'exécution des décisions judiciaires pénales restrictives ou privatives de libertés par les organismes habilités ;
- assister les personnes dans le cadre des démarches pour l'obtention d'une domiciliation pour les personnes sans domicile stable ;
- assister les personnes dans le cadre des démarches administratives nécessaires aux procédures de demandes d'asile (p. ex. : traduction, information et accompagnement quant aux recours en cas de refus de la demande etc.) ;
- assister les personnes dans le cadre des démarches auprès des créanciers privés et/ou publics (p. ex. : assistance dans le cadre des procédures de surendettement auprès de la Banque de France, etc.).

d) d'échanger et de partager les informations strictement nécessaires, dans le respect des dispositions de l'article L. 1110-4 du CSP et des dispositions du CASF, permettant de garantir la coordination et la continuité de l'accompagnement et du suivi des personnes entre les intervenants sociaux, médicaux et paramédicaux ;

e) d'assurer la gestion administrative (nombre de places disponibles, capacité d'accueil de l'établissement, etc.)**, financière et comptable** de l'établissement, du service ou de l'organisme ;

> **Attention :** S'agissant de la gestion administrative du personnel, les organismes peuvent utilement se référer au référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel disponible sur le site web de la Commission.

f) **d'assurer la remontée des informations préalablement anonymisées aux autorités compétentes** 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 conformément aux dispositions des articles R. 331-8 et suivants du CASF**, établir des statistiques, des études internes et des enquêtes de satisfaction** aux fins d'évaluation de la qualité des activités et des prestations et des besoins à couvrir**.**

> **Attention :** Dès lors que ces statistiques, études et évaluations entrent dans le champ des recherches, études et évaluations dans le domaine de la santé, les traitements constitués devront respecter les dispositions des articles 72 et suivants de la loi « Informatique et Libertés ».

Les informations recueillies pour l'une de ces finalités ne peuvent pas en principe être réutilisées pour poursuivre un objectif qui serait incompatible avec la finalité initiale. Tout nouvel usage des données doit en effet respecter les principes de protection des données à caractère personnel, en particulier le principe de finalité des traitements (par exemple, les traitements mis en œuvre pour les finalités énoncées ci-dessus ne doivent pas donner lieu à des interconnexions ou échanges autres que ceux nécessaires à l'accomplissement de celles-ci).

4. Base(s) légale(s) du traitement

Chaque finalité du traitement doit reposer sur l'une des bases légales fixées par la réglementation (article 6 du RGPD). (voir pour une explicitation de cette règle : « la licéité du traitement : l'essentiel sur les bases légales prévues par le RGPD »).

Il appartient au responsable de traitement de déterminer ces bases légales avant toute opération de traitement, après avoir mené une réflexion, qu'il pourra documenter, au regard de sa situation spécifique et du contexte. Ayant un impact sur l'exercice de certains droits, ces bases légales font partie des informations devant être portées à la connaissance des personnes concernées.

Le tableau reproduit ci-dessous vise à apporter aux responsables de traitement une aide pour identifier les bases légales susceptibles d'être utilisées dans les cas les plus courants.

Ces éléments doivent être adaptés à la situation spécifique de chaque organisme concerné. Ainsi, par exemple, selon que l'organisme en question relève du secteur privé ou public, certains traitements répondant pourtant à la même finalité (par exemple, ceux liés à la gestion administrative des personnes suivies, accueillies ou hébergées) peuvent être fondés sur des bases légales différentes (par exemple, intérêt légitime dans le secteur privé, exécution d'une mission d'intérêt public dans le secteur public).

Attention : dans le cadre de l'accompagnement social et/ou médico-social des personnes âgées, en situation de handicap ou en difficulté, la commission appelle l'attention des organismes sur la nécessité de faire preuve de la plus grande prudence dans l'usage du consentement comme base légale de leurs traitements de données à caractère personnel. Les personnes concernées peuvent en effet souffrir d'altération du discernement pouvant rendre le consentement non valable.

En outre, il est rappelé que la personne concernée qui fournit son consentement peut à tout moment le retirer, mettant fin en principe à la possibilité de traiter les données la concernant pour l'avenir.

De manière générale, le responsable de traitement doit veiller au respect des conditions de recueil du consentement et plus particulièrement au caractère libre, spécifique, éclairé et univoque du consentement.

<table>
<tr><th>Finalités</th><th colspan="2">Bases légales envisageables
(sous réserve de choix différents justifiés par un contexte spécifique qu'il est recommandé de documenter)</th></tr>
<tr><td rowspan="2">Fourniture des prestations définies dans le cadre du contrat conclu entre l'organisme et la personne concernée ou son représentant légal et, le cas échéant, gestion administrative des personnes concernées</td><td colspan="2">Organismes publics ou personnes morales de droit privé gérant un service public

Exécution du contrat ou mission d'intérêt public dès lors que le traitement mis en œuvre excède ce qui est nécessaire au contrat</td></tr>
<tr><td colspan="2">Organismes privés

Exécution du contrat ou intérêts légitimes dès lors que le traitement mis en œuvre excède ce qui est nécessaire au contrat</td></tr>
<tr><td rowspan="3">Accompagnement social et médico-social adapté aux difficultés rencontrées ayant notamment pour objet d'élaborer un projet personnalisé d'accompagnement, d'assurer le suivi des personnes dans l'accès aux droits et, le cas échéant, d'orienter les personnes vers les structures compétentes susceptibles de les prendre en charge</td><td colspan="2">Organismes publics ou personnes morales de droit privé gérant un service public

Mission d'intérêt public</td></tr>
<tr><td colspan="2">Organismes privés

Intérêts légitimes</td></tr>
<tr><td>Cas particulier s'agissant du suivi des personnes et des familles reçues dans le cadre de la médiation familiale, sociale ou pénale, à l'exclusion des mesures relevant de l'aide sociale à l'enfance et du suivi de l'exécution des décisions judiciaires pénales restrictives ou privatives de libertés par les organismes habilités</td><td>Obligation légale, sous réserve du respect des dispositions de l'article 46 de la loi « Informatique et Libertés » relatif aux condamnations pénales, infractions et mesures de sûreté</td></tr>
</table>

<table>
<tr><td></td><td colspan="2">Cas particulier concernant les droits relatifs à la fin de vie</td><td>Consentement</td></tr>
<tr><td rowspan="3">Instruction, gestion et, le cas échéant, ouverture des droits et/ou versement des demandes de prestations sociales légales ou facultatives</td><td>Aides légales</td><td colspan="2">Mission d’intérêt public</td></tr>
<tr><td rowspan="2">Aides facultatives</td><td colspan="2">Organismes publics ou personnes morales de droit privé gérant un service public

Mission d’intérêt public</td></tr>
<tr><td colspan="2">Organismes privés

Intérêts légitimes</td></tr>
<tr><td rowspan="2">Échange et partage des informations strictement nécessaires permettant de garantir la coordination et la continuité de l’accompagnement et du suivi des personnes entre les intervenants sociaux, médicaux et paramédicaux</td><td colspan="3">Organismes publics ou personnes morales de droit privé gérant un service public

Mission d’intérêt public</td></tr>
<tr><td colspan="3">Organismes privés

Intérêts légitimes</td></tr>
<tr><td rowspan="2">Gestion administrative, financière et comptable de l’établissement, du service ou de l’organisme</td><td colspan="3">Organismes publics ou personnes morales de droit privé gérant un service public

Obligation légale (p. ex. : décret n° 2012-1246 du 7 novembre 2012 relatif à la gestion budgétaire et comptable publique, etc.)</td></tr>
<tr><td colspan="3">Organismes privés

Obligation légale (p. ex. : règlement n° 2018-06 du 5 décembre 2018 relatif aux comptes annuels des personnes morales de droit privé à but non lucratif, etc.)</td></tr>
<tr><td>Remontée des informations préalablement anonymisées aux autorités compétentes concernant des dysfonctionnements graves, établissement des statistiques, des études internes et des enquêtes de satisfaction aux fins d’évaluation des activités,</td><td colspan="3">Organismes publics ou personnes morales de droit privé gérant un service public

Obligation légale (p. ex. : les dispositions de l’article L. 232-17 du CASF prévoient la transmission au ministre en charge des personnes âgées, des données statistiques relatives au développement du dispositif de l’APA ; les dispositions de l’article L. 345-2-4 du CASF encadrent la production de données statistiques d’activité, de suivi et de pilotage d’accueil, d’hébergement et d’accompagnement vers l’insertion et le logement pour les services intégrés d’accueil et d’orientation, etc.) ou mission d’intérêt public</td></tr>
</table>

de la qualité des prestations et des besoins à couvrir	**<u>Organismes privés</u>** Obligation légale (p. ex. : la remontée des informations préalablement anonymisées aux autorités compétentes 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 conformément aux dispositions des articles R. 331-8 et suivants du CASF) ou intérêts légitimes

5. Données à caractère personnel concernées

5.1. Principes de pertinence et de minimisation des données

En vertu du principe de minimisation des données, le responsable de traitement doit veiller à ce que **seules les données nécessaires à la poursuite des finalités du traitement soient effectivement collectées et traitées**. Sont en principe considérées comme pertinentes, pour les finalités rappelées ci-dessus, les catégories de données suivantes relatives :

a) à l'identification des bénéficiaires de l'accompagnement social et médico-social et, le cas échéant, de leurs représentants légaux ;

b) à la vie personnelle ;

c) au parcours professionnel et de formation dans le cadre de l'aide à l'insertion professionnelle des personnes ;

d) aux conditions de vies matérielles ;

e) à la couverture sociale ;

f) aux coordonnées bancaires dans la mesure où cette information est nécessaire au versement d'une prestation ;

g) à l'évaluation sociale et médico-sociale de la personne concernée ;

h) au type d'accompagnement et aux actions mis en œuvre ;

i) à l'identification des personnes concourant à la prise en charge sociale et médico-sociale et à l'entourage susceptible d'être contacté ;

j) à l'identification des personnes dans le cadre de l'accompagnement au numérique.

De manière générale, le responsable de traitement ne doit collecter que les données dont il a **réellement besoin** et ne doit le faire qu'à partir du moment où ce besoin se concrétise.

Exemples :

Peuvent être collectés **la nationalité du bénéficiaire sous la forme « Français / UE / hors UE »** et les documents prouvant la régularité de son séjour en France, dès lors que le bénéfice de l'aide ou de la prestation sollicitée est soumis à une condition de régularité du séjour.

Dans le cadre de l'accompagnement relatif à la demande d'asile et/ou à la demande d'un titre de séjour, peuvent être collectées les informations relatives à la procédure de demande d'asile sous la forme « dépôt d'une demande d'asile oui/non » et/ou les informations relatives à la procédure de demande de titre de séjour sous la forme « dépôt d'une demande de titre de séjour oui/non », **la nationalité de la personne concernée** ainsi que **les informations nécessaires à l'élaboration du récit de vie.**

5.2. Le traitement du numéro de sécurité sociale (NIR), des données sensibles et des données relatives aux condamnations pénales et aux infractions

Certaines catégories de données appellent, une vigilance renforcée en raison de leur caractère particulièrement sensible. Bénéficiant d'une protection spécifique, elles ne peuvent être collectées et traitées que dans des conditions strictement définies par les textes. Il s'agit :

- **du NIR**, qui fait l'objet d'une réglementation spécifique et ne peut, être enregistré dans le traitement que dans le cadre des échanges avec les professionnels de santé ou les organismes de sécurité sociale, de prévoyance et les MDPH. A cet égard, le **décret en Conseil d'Etat n° 2019-341 du 19 avril 2019** pris après avis de la CNIL, détermine les catégories de responsables de traitement et les finalités de ces traitements au vu desquelles ces derniers peuvent être mis en œuvre lorsqu'ils portent sur des données comportant le NIR (voir aussi « Tout savoir sur le décret « cadre NIR » dans le champ de la protection sociale ») ;

- **de l'identifiant national de santé ou INS (articles L. 1111-8-1 et R. 1111-8-1 et suivants du code de la santé publique)** qui ne peut être utilisé que pour répertorier et retrouver les données de santé et les données administratives rattachées à une personne bénéficiant ou appelée à bénéficier d'une prise en charge sanitaire ou médico-sociale. L'INS ne peut être utilisé que par les professionnels, les établissements, services ou organismes participant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le CSP (professionnels de santé libéraux, établissements de santé, etc.), par les professionnels du secteur social et médico-social, par les établissements ou services sociaux ou médico-sociaux (p. ex. : maisons de retraite, MDPH, etc.) ou par les professionnels constituant une équipe de soins au sens de l'article L. 1110-12 du CSP et intervenant dans la prise en charge sanitaire ou médico-sociale de l'usager ;

- **des données relatives aux infractions, condamnations pénales et mesures de sûreté connexes qui ne peuvent être traitées que dans certains cas dans le respect des dispositions légales relatives aux données d'infractions (art. 46 de la LIL) ;**

> **Par exemple** si :
> - elles sont strictement nécessaires dans le cadre des actions mises en œuvre en faveur des personnes détenues ou placées sous main de justice, d'une part, et dans le cadre de l'aide et du soutien des victimes d'infractions ou des familles de personnes détenues ;
> - elles permettent d'établir l'existence d'une situation de maltraitance passée ou en cours afin d'adapter l'accompagnement de la personne concernée (p. ex. : l'accompagnement des femmes victimes de violences conjugales par une association d'aide aux victimes agréée par le ministère de la justice conformément aux dispositions de l'article 46 al. 1 de la loi Informatique et Libertés et de l'article 76 du décret n° 2019-536 du 29 mai 2019).

- **des données dites « données sensibles »**, c'est-à-dire celles qui révèlent l'origine ethnique ou prétendument raciale, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne, les données génétiques, les données biométriques, les données concernant la santé ou celles concernant la vie sexuelle ou l'orientation sexuelle d'une personne. Ces données ne peuvent pas être collectées, sauf exception prévue par les textes.

À titre d'exemple, peuvent être collectées des données relatives à **la santé, sous réserve que ces données soient collectées à des fins** :

- d'administration de soins, de traitements, de diagnostics médicaux, de médecine préventive ou de gestion des services de santé. Les traitements au sein desquels ces données sont intégrées doivent être mis en œuvre par un membre d'une profession de santé ou par une autre personne à laquelle s'impose en raison de ses fonctions, l'obligation de secret professionnel dont l'atteinte est réprimée par l'article 226-13 du code pénal ;
- ou de délivrance d'une prestation sociale destinée aux personnes en situation de perte d'autonomie ou de handicap prévue par un texte législatif ou réglementaire, sous réserve que ces informations soient strictement nécessaires à la délivrance de ladite prestation.

Lorsque la collecte de données de santé est nécessaire à l'accompagnement social réalisé mais ne s'inscrit pas au sein de l'une des deux situations susvisées, celle-ci peut être réalisée après recueil du consentement de la personne concernée ou de son représentant légal (p. ex. : une aide à domicile peut recevoir communication de l'état de santé d'une personne dès lors que ces informations sont nécessaires à l'accompagnement social et médico-social réalisé à domicile). À cet égard, le responsable de traitement doit veiller au respect des conditions de recueil du consentement et plus particulièrement au caractère libre, spécifique, éclairé et univoque du consentement.

Peuvent également être collectées les données relatives **aux convictions religieuses et/ou philosophiques sous réserve (conditions cumulatives)** :

- d'être collectées auprès de la personne concernée ou de son représentant légal, après recueil du consentement exprès. De la même manière, le responsable de traitement doit veiller au respect des conditions de recueil du consentement et plus particulièrement au caractère libre, spécifique, éclairé et univoque du consentement ;
- et d'être strictement nécessaires à l'accompagnement social et/ou médico-social (p. ex. : organisation des repas, des funérailles, accompagnement des personnes victimes ou susceptibles d'être victimes de mouvements extrémistes etc.).

Il convient de distinguer le consentement en tant qu'exception prévue par le RGPD autorisant la collecte de données sensibles, du consentement en tant que base légale ou base juridique qui autorise légalement la mise en œuvre du traitement.

Exemple :

Dans le cadre de l'accompagnement social et médico-social adapté aux difficultés rencontrées des personnes, des données sensibles, notamment les convictions religieuses, sont susceptibles d'être collectées par le responsable de traitement. Par conséquent, si la base légale du traitement repose sur l'intérêt légitime, l'exécution du contrat ou la mission d'intérêt public, un consentement spécifique devra être recueilli pour pouvoir traiter les informations relatives aux convictions religieuses.

Le tableau reproduit ci-dessous fournit des illustrations des données que la CNIL considère comme étant en principe adaptées selon les finalités du traitement.

Catégories de données	Exemples de données
À l'identification des bénéficiaires de l'accompagnement social et médico-social et, le cas	Nom, prénom, sexe, adresse, courriel, numéro de téléphone, date et lieu de naissance, photographie. La photographie ne doit être collectée que lorsque cela est strictement nécessaire au regard de l'objectif poursuivi (p. ex. : pour retrouver un pensionnaire d'un EHPAD qui s'est soustrait à la vigilance du personnel).

échéant, de leurs représentants légaux	**Numéro d'identification de rattachement à un organisme** : numéro d'adhérent ou d'allocataire.
	Numéro de sécurité sociale dans les conditions fixées par le décret n° 2019-341 du 19 avril 2019.
	Nationalité du bénéficiaire sous la forme « Français / UE / hors UE », les documents prouvant la régularité du séjour en France de la personne concernée dès lors que le bénéfice de l'aide ou de la prestation sociale est soumis à une condition de régularité du séjour. **Informations relatives à la procédure de demande d'asile** sous la forme « dépôt d'une demande d'asile : oui/non » et/ou **à la procédure de demande de titre de séjour** sous la forme « dépôt d'une demande de titre de séjour oui/non », **la nationalité** de la personne concernée ainsi que les informations nécessaires à l'élaboration du récit de vie de la personne concernée.
	Dans des cas exceptionnels, la photocopie de la pièce d'identité de la personne concernée notamment dans le cadre de l'accompagnement relatif à la gestion budgétaire auprès des organismes publics et/ou privés (p. ex. : dépôt d'un dossier de surendettement auprès de la Banque de France, etc.).
À la vie personnelle	Situation et composition familiale du foyer, le cas échéant, l'identification d'enfants pris en charge dans le cadre de la protection de l'enfance, habitudes de vie nécessaires à l'organisation de la vie quotidienne (p. ex. : habitudes alimentaires, activité physique, toilette quotidienne, nombre d'heure de sommeil, etc.), centres d'intérêt, langue parlée dans la mesure où cette information est indispensable pour mentionner le besoin d'interprètes.
Au parcours professionnel et de formation dans le cadre de l'aide à l'insertion professionnelle des personnes	Scolarité, situation au regard de l'emploi, de la formation et de la qualification.
Aux conditions de vie matérielles	**Situation financière** : ressources, charges, crédits, dettes. Peuvent également être collectées les informations relatives à la **liste des comptes bancaires existants, aux dates d'ouverture desdits comptes, aux moyens de paiement, au montant du découvert autorisé ainsi qu'à l'inscription, le cas échéant, au fichier national des incidents de remboursement des crédits aux particuliers (FICP) et au fichier central des chèques (FCC)** sous réserve que ces informations soient strictement nécessaires à l'accompagnement budgétaire réalisé.
	Prestations et avantages sociaux perçus : nature, montant, quotient familial, numéro d'allocataire.
	Situation face au logement et à l'hébergement : type et caractéristiques du logement ou modalités d'hébergement (domicile personnel, familial, sans abri, hébergement de fortune, hébergement mobile, hébergement d'urgence, hébergement d'insertion).
	Moyens de mobilité.

À la couverture sociale	Organismes de rattachement et régimes d'affiliation, droits ouverts.
Aux coordonnées bancaires dans la mesure où cette information est nécessaire au versement d'une prestation	Relevé d'identité bancaire (RIB).
À l'évaluation sociale et médico-sociale de la personne concernée	Difficultés rencontrées et appréciations sur celles-ci, évaluation de la situation des personnes afin de repérer l'aggravation de difficultés ou encore d'une perte d'autonomie s'agissant des personnes âgées ou en situation de handicap.
Au type d'accompagnement et aux actions mis en œuvre	Domaines d'intervention, historique des mesures d'accompagnement, objectifs, parcours, actions d'insertion prévues, entretien et suivi.
À l'identification des personnes concourant à la prise en charge sociale et médico-sociale et à l'entourage susceptible d'être contacté	Nom, prénom, qualité, organisme d'appartenance, numéro de téléphone de l'organisme, adresse, courriel, numéro de téléphone des aidants professionnels ou familiaux (le cas échéant, le lien familial : époux / épouse, frère / sœur, fils / fille, etc.), du médecin traitant, des médecins experts, de la personne de confiance.
À l'identification des personnes dans le cadre de l'accompagnement au numérique	Dans des cas exceptionnels, il est possible d'enregistrer les **identifiants et mots de passe de l'espace personnel de la personne concernée** lorsque celle-ci n'est pas en capacité de se connecter seule (p. ex. : la personne concernée n'est pas en mesure de se déplacer et est dépourvue d'un accès à Internet). **L'enregistrement des mots de passe de l'usager ne doit être réalisé que dans le cadre d'un mandat signé entre l'usager et le professionnel** (voir exemple de mandat disponible sur le site web de la CNIL). S'agissant du choix du mot de passe, la CNIL conseille vivement de se conformer à la délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe modifiée.
Informations relatives à certaines aides sociales légales (liste non exhaustive)	**Aide sociale pour l'hébergement (ASH) et allocation personnalisée d'autonomie (APA) :** les données susceptibles d'être collectées par les conseils départementaux dans le cadre de l'instruction, la gestion et le versement de l'APA et de l'ASH sont listées par l'article R. 232-41 du CASF.
	Carte « mobilité inclusion » : les données susceptibles d'être collectées par les MDPH et les conseils départementaux dans le cadre de l'instruction, la gestion et la délivrance des cartes « mobilité inclusion » sont listées par l'article D. 241-18-1 du CASF.
	Revenu de solidarité active (RSA) : les données susceptibles d'être collectées par les caisses d'allocations familiales (CAF) et les caisses de mutualité sociale agricole (MSA) dans le cadre de l'instruction, la liquidation et le versement du RSA sont listées à l'article R. 262-103 du CASF. Les informations relatives aux bénéficiaires du RSA font l'objet d'échanges entre les conseils départementaux et Pôle emploi afin de coordonner leurs actions d'insertion

	professionnelles conformément aux dispositions de l'article R. 262-116-2 du CASF.

Après s'être assuré de la pertinence et de la proportionnalité des données à caractère personnel qu'il traite, l'organisme doit par ailleurs s'assurer, tout au long de la durée de vie du traitement, de la qualité de ces données qui doivent être exactes, mises à jour et toujours nécessaires à l'objectif poursuivi.

6. Destinataires des données et accès aux informations

Les données personnelles ne peuvent être rendues accessibles qu'aux seules personnes habilitées à en connaitre au regard de leurs attributions.

D'une manière générale, les habilitations d'accès doivent être documentées par les organismes, et les accès aux différents traitements doivent faire l'objet de mesures de traçabilité. **Voir point 10 relatif à la sécurité.**

Sauf cas particuliers, le partage des informations collectées devrait notamment respecter les principes suivants :

- les informations échangées ne doivent servir qu'à évaluer la situation de la personne ou de la famille concernée afin de déterminer les actions à mettre en œuvre ;
- ces échanges d'informations doivent en outre être strictement limités à l'accomplissement des missions de l'organisme ou du service mettant en œuvre le traitement ;
- ils ne peuvent pas porter sur l'ensemble des informations dont les intervenants sont dépositaires mais doivent être limités à celles nécessaires à l'accompagnement et au suivi des personnes, dans le respect de leur vie privée ;
- les échanges doivent être réalisés dans les conditions fixées par les textes législatifs et réglementaires.

6.1. Les personnes accédant aux données pour le compte du responsable de traitement

Seules les personnes habilitées au titre de leurs missions ou de leurs fonctions peuvent accéder aux données à caractère personnel traitées, et ce dans la stricte limite de leurs attributions respectives et de l'accomplissement de ces missions et fonctions.

Il peut s'agir, par exemple, des professionnels et de tout membre du personnel de l'établissement, du service concourant à une ou plusieurs des finalités susvisées, dans la limite de leurs attributions respectives et des règles encadrant le partage et l'échange d'informations (p. ex. : l'équipe pluridisciplinaire des MDPH visée par les dispositions de l'article L. 146-8 du CASF, les professionnels et tout membre du personnel membre de la même équipe de soins exerçant au sein du même établissement, etc.).

6.2. Les destinataires des données

Le RGPD définit les destinataires comme « *tout organisme qui reçoit la communication des données* ».

Avant toute communication des informations, le responsable de traitement doit d'une part, s'interroger sur la finalité de la transmission pour s'assurer de sa pertinence et de sa légitimité et, d'autre part,

vérifier que les données communiquées sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie.
Dans le cadre de ce référentiel, peuvent **notamment** être destinataires des données **(liste non exhaustive)** :

- s'agissant de données traitées par une personne soumise au secret médical/professionnel, les professionnels et tout membre du personnel membre de la même équipe de soins ou non et n'exerçant pas au sein du même établissement, sous réserve dans ce dernier cas du recueil du consentement de la personne concernée conformément aux dispositions de l'article L. 1110-4 du CSP, qui participent à une ou plusieurs des finalités susvisées ;

- les personnes appelées à intervenir dans la gestion financière et successorale du patrimoine de la personne ayant fait l'objet d'un accompagnement et d'un suivi ;

- les organismes instructeurs et payeurs de prestations sociales ;

- les organismes financeurs et gestionnaires, s'agissant exclusivement de données préalablement anonymisées, à l'exception de ceux autorisés par une disposition légale ou réglementaire à obtenir la communication de données à caractère personnel des personnes accompagnées ;

- les autorités administratives compétentes mentionnées par les dispositions des articles R. 331-8 et suivants du CASF, s'agissant exclusivement de données préalablement anonymisées, dans le cadre des signalements de dysfonctionnement grave ou évènement ayant pour effet de menacer ou de compromettre la santé, la sécurité ou le bien-être des personnes prises en charge.

6.3. Les sous-traitants

Le RGPD définit les sous-traitants comme « *La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ».

Il peut s'agir, par exemple, des prestataires de services informatiques (hébergement, maintenance, etc.) ou encore de tout organisme offrant un service ou une prestation impliquant un traitement de données à caractère personnel pour le compte d'un autre organisme (p. ex. : la gestion de la paie des salariés ou des agents, etc.).

Le responsable de traitement qui souhaite avoir recours à un sous-traitant doit veiller à ne faire appel qu'à des organismes présentant des garanties suffisantes. Un contrat définissant les caractéristiques du traitement ainsi que les différentes obligations des parties en matière de protection des données doit être établi entre elles (article 28 du RGPD).

Pour en savoir plus, un guide du « sous-traitant », édité par la CNIL, rappelle ces obligations et donne des exemples de clauses à intégrer dans les contrats.

6.4. Les tiers autorisés

Les autorités légalement habilitées sont susceptibles, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, de demander au responsable de traitement la communication de données à caractère personnel (p. ex. : Pôle emploi ou les organismes de sécurité sociale dans le cadre de la lutte contre la fraude, les administrations de la justice, de la police, de la gendarmerie, etc.).

Dans ce cas, le responsable du traitement doit s'assurer du caractère contraignant de la disposition avancée et ne transmettre que les données prévues par le texte, ou, si ce dernier ne les liste pas, les seules données indispensables au regard de la finalité du droit de communication en question.

Pour en savoir plus, l'organisme a la possibilité de consulter le guide pratique « tiers autorisés » sur le site web de la CNIL.

6.5. Les transferts de données à caractère personnel en dehors de l'Union européenne

Pour assurer la continuité de la protection des données à caractère personnel, leur transfert en dehors de l'Union européenne est soumis à des règles particulières. Ainsi, conformément aux dispositions des articles 44 et suivants du RGPD, toute transmission de données hors de l'UE doit :

- être fondée sur une décision d'adéquation ;
- ou être encadrée par des règles internes d'entreprise (« BCR »), des clauses types de protection des données, un code de conduite ou un mécanisme de certification approuvé par la CNIL ;
- ou être encadrée par des clauses contractuelles *ad hoc* préalablement autorisées par la CNIL ;
- ou répondre à une des dérogations prévues à l'article 49 du RGPD.

Pour en savoir plus, l'organisme a la possibilité de consulter la rubrique « Transférer des données hors de l'UE » sur le site web de la CNIL.

7. Durées de conservation

Une durée de conservation précise des données doit être fixée en fonction de chaque finalité : ces données ne peuvent en effet pas être conservées pour une durée indéfinie.

La durée de conservation de données ou, lorsqu'il est impossible de la fixer, les critères utilisés pour déterminer cette durée, font partie des informations qui doivent être communiquées aux personnes concernées.

Dans ces conditions, il incombe au responsable du traitement de déterminer cette durée en amont de la réalisation du traitement.

7.1 Les durées de conservation

En principe, il est recommandé que les données collectées et traitées, pour les besoins de l'accueil, l'hébergement et l'accompagnement social et médico-social des personnes ne soient pas conservées dans la base active au-delà de deux ans à compter du dernier contact émanant de la personne ayant fait l'objet de cet accompagnement (p. ex. : dernier courriel ou courrier envoyé par la personne concernée, etc.), sauf dispositions législatives ou réglementaires contraires ou cas particulier. **Cette durée de conservation est celle préconisée par la Commission s'agissant de l'ensemble des finalités visées par le référentiel.**

Les données peuvent en outre être conservées plus longtemps que les durées mentionnées ci-dessus, en archivage intermédiaire, dans certains cas particuliers, par exemple **si le responsable du traitement en a l'obligation légale** (par exemple, pour répondre à des obligations comptables, sociales ou fiscales) ou **s'il a besoin de se constituer une preuve en cas de contentieux** et dans la limite du délai de prescription/forclusion applicable (par exemple, en matière de discrimination). La **durée de l'archivage intermédiaire doit cependant répondre à une réelle nécessité, dûment justifiée par le responsable de traitement** après une analyse préalable de différents facteurs, notamment le contexte, la nature des données traitées et le niveau de risque d'un éventuel contentieux.

À l'expiration de ces périodes, les données sont détruites de manière sécurisée ou archivées dans des conditions définies en conformité avec les dispositions du code du patrimoine relatives aux obligations d'archivage des informations du secteur public pour les organismes soumis à ces dispositions, d'une part, ou conformément aux dispositions de la délibération de la CNIL portant adoption d'une recommandation concernant les modalités d'archivage électronique de données à caractère personnel pour les organismes relevant du secteur privé, d'autre part.

Le tableau suivant contient des exemples pour lesquels la durée de conservation est en principe adéquate au regard des textes (**liste non exhaustive**) :

Activités de traitement	Détails du traitement	Base active	Archivage intermédiaire	Textes de référence
Instruction gestion et versement des prestations sociales légales	APA/ASH	Six ans après la cessation de son droit à la prestation ou après l'intervention d'une décision définitive en cas de contentieux	À des fins de pilotage départemental concernant la connaissance de la population des demandeurs et bénéficiaires de l'APA et de l'ASH ainsi que pour la constitution d'échantillons statistiquement représentatifs prévue à l'article L. 232-21-2 du CASF, visant à rendre possible l'étude des situations et des parcours des personnes y compris lorsqu'elles changent de département, les données peuvent être conservées au-delà du délai de six ans, liées à un numéro d'anonymat	Art. R. 232-46 du CASF
	Dans le cadre des échanges de données entre Pôle emploi et le conseil départemental pour l'orientation et l'accompagnement des bénéficiaires du RSA	Deux mois au maximum à compter de la transmission des informations	Trois ans à compter de la transmission des informations à Pôle emploi	Art. R. 262-116-4 du CASF
Instruction gestion et délivrance de la carte « mobilité inclusion »	Carte « mobilité inclusion »	Cinq ans à compter de la date d'expiration de validité de la dernière décision intervenue ou pendant laquelle aucune intervention n'a été enregistrée dans le	Au-delà de cette période, les informations sorties du système de traitement sont archivées sur un support distinct et peuvent être conservées dix ans dans des conditions de sécurité équivalentes à celles des autres données enregistrées dans le traitement	Art. 241-19-3 du CASF

		dossier de la personne		
Accompagnement médico-social de la personne concernée	Dossier médical	Deux ans à compter du dernier contact avec la personne concernée	Vingt ans à compter de la date du dernier séjour de son titulaire au sein de l'établissement de sa prise en charge Si la personne titulaire du dossier décède moins de dix ans après son dernier passage dans l'établissement, le dossier est conservé pendant une durée de dix ans à compter de la date du décès.	Art. R. 1112-7 du CSP

7.2 La conservation de données anonymisées

La réglementation relative à la protection des données à caractère personnel ne s'applique pas, notamment en ce qui concerne les durées de conservation, aux **données anonymisées.** Il s'agit des données qui ne peuvent plus, par quiconque, être mises en relation avec la personne physique identifiée à laquelle elles se rapportaient initialement.

L'anonymisation doit être distinguée de la pseudonymisation où il est techniquement possible de retrouver l'identité de la personne concernée grâce à des données tierces. En effet, l'opération de pseudonymisation est réversible, contrairement à l'anonymisation.

Ainsi, le responsable du traitement peut conserver sans limitation de durée les données anonymisées. Dans ce cas, l'organisme concerné doit garantir le caractère anonymisé des données de façon pérenne.

Pour en savoir plus, l'organisme a la possibilité de consulter les guides de la CNIL suivants :

- « Sécurité : Archiver de manière sécurisée » ;
- « Limiter la conservation des données » ;
- « Guide pratique : les durées de conservation ».

L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et ce de manière irréversible. Aussi, une fois anonymisées, les données ne peuvent plus être reliées à une personne (Pour en savoir plus, vous pouvez vous référer aux lignes directrices du CEPD sur l'anonymisation).

8. Information des personnes

Un traitement de données à caractère personnel doit être mis en œuvre en toute transparence vis-à-vis des personnes concernées.

8.1 Contenu de l'information à délivrer

L'information communiquée aux personnes doit se faire dans les conditions prévues par les articles 12, 13 et 14 du RGPD.

Dès le stade de la collecte des données à caractère personnel, les personnes concernées doivent notamment être informées de **l'existence du traitement, de ses caractéristiques essentielles**

(parmi lesquelles l'identité du responsable du traitement et l'objectif poursuivi) et des droits dont elles disposent.

Des exemples de mentions d'information sont disponibles sur le site de la CNIL et peuvent être consultés dans la rubrique « RGPD : exemples de mentions d'information ».

8.2 Les modalités de l'information

Afin de respecter pleinement les principes de loyauté et de transparence et conformément aux dispositions des articles 13 et 14 du RGPD, les personnes doivent en principe être directement informées au moment où les données sont collectées.

Si le RGPD n'impose aucune forme spécifique, **une information écrite doit être privilégiée de manière à pouvoir justifier de son contenu**, ainsi que du moment où elle a été délivrée.

Dans le cadre de l'accompagnement social et médico-social des personnes, le responsable de traitement procède à l'information des personnes concernées et, le cas échéant, de leurs représentants légaux par tout moyen approprié (p. ex. : mentions d'informations insérées au sein du livret d'accueil, du contrat de séjour, du DIPEC, du contrat d'hébergement, des formulaires de demandes de prestations sociales, etc.), dans un langage compréhensible et selon des modalités appropriées et adaptées à leur situation (p. ex. : pictogramme, à l'oral, images ludiques notamment lorsque le public concerné est mineur, recours à la méthode « Facile à lire et à comprendre » dite « FALC », etc.) conformément aux dispositions de l'article 12 du RGPD. De manière générale, la Commission recommande une information orale en plus d'une information écrite afin de s'assurer de la bonne compréhension par la personne concernée des informations communiquées.

9. Droits des personnes

Les personnes concernées disposent des droits suivants, qu'elles exercent dans les conditions prévues par le RGPD (pour aller plus loin voir la rubrique qui s'intitule « Comprendre mes droits » sur le site de la CNIL) :

- le **droit d'accès,** permet à la personne concernée de savoir si des données la concernant sont traitées par le responsable de traitement et, dans cette hypothèse, d'obtenir des précisions sur les conditions de ce traitement et, à sa demande, d'obtenir une copie des données la concernant détenues par ce responsable ;

- **le droit de rectification,** permet à la personne concernée de demander la rectification des informations inexactes ou incomplètes la concernant ;

- **le droit à l'effacement**, permet à la personne concernée de demander à un organisme l'effacement de données à caractère personnel la concernant (p. ex. : les données sont effacées par le responsable de traitement pour respecter les délais de conservation fixés par les textes législatifs ou réglementaires, la personne a retiré le consentement sur lequel est fondé le traitement, etc.) ;

- le **droit à la limitation** du traitement (par exemple, lorsque la personne conteste l'exactitude de ses données, celle-ci peut demander à l'organisme le gel temporaire du traitement de ses données, le temps que celui-ci procède aux vérifications nécessaires) ;

- le **droit à la portabilité**, dans les conditions prévues conformément aux dispositions du RGPD, offre à la personne concernée la possibilité de récupérer une partie des données la concernant dans un format ouvert et lisible par machine afin de les réutiliser à des fins personnelles. Ce droit ne s'applique que si les trois conditions suivantes sont réunies : limitation aux seules données à caractère personnel fournies par la personne concernée ; application uniquement si les données sont traitées de manière automatisée (exclusion des fichiers par voie papier) et sur la base du consentement préalable de la personne concernée ou de l'exécution d'un contrat conclu avec la personne concernée ; respect des droits et libertés de tiers ;
- le **droit de s'opposer au traitement** de leurs données, sous réserve des conditions d'exercice

de ce droit en application des dispositions de l'article 21 du RGPD.
En ce qui concerne les traitements relatifs à l'accompagnement social et/ou médico-social, la personne concernée pourra s'opposer au traitement de ses données, à condition d'invoquer des raisons tenant à sa situation particulière, et 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 ou d'une mission relevant de l'exercice de l'autorité publique (p. ex. : le responsable de traitement peut refuser à la personne concernée l'exercice de son droit d'opposition dès lors que le traitement des informations la concernant repose sur l'obligation légale).

Le responsable du traitement pourra refuser de donner suite à cette demande d'opposition s'il démontre qu'il dispose d'intérêts légitimes et impérieux qui prévalent sur les droits et libertés du demandeur.

Attention : Le responsable du traitement doit répondre aux demandes reçues dans les meilleurs délais et dans un délai d'un mois maximum. Si un délai supplémentaire est nécessaire pour traiter la demande (par exemple, en raison de sa complexité), la personne concernée doit en être informée dans ce même délai d'un mois. Dans tous les cas, une réponse doit être apportée dans un délai qui ne peut pas dépasser trois mois.

L'exercice des droits par les personnes doit être facilité par le responsable de traitement et être gratuit. Les personnes concernées doivent être informées de leur possibilité d'adresser une réclamation à la Commission nationale de l'informatique et des libertés si elles ne sont pas satisfaites du traitement de leurs données à caractère personnel.

10. Sécurité

L'organisme doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel et, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

En particulier, dans le contexte spécifique de ce référentiel, **l'organisme est invité à mettre en œuvre les mesures suivantes, ou être en mesure de justifier de la mise en place de mesures équivalentes ou de leur absence de nécessité ou de possibilité** (les particuliers traitant un volume faible de données prennent, par exemple, les mesures élémentaires de sécurité pour assurer la sécurité et la confidentialité des données qu'ils traitent) :

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser les personnes manipulant les données
	Rédiger une charte informatique et lui donner une force contraignante
Authentifier les utilisateurs	Définir un identifiant (*login*) unique à chaque utilisateur
	Adopter une politique de mots de passe utilisateur conforme aux recommandations de la CNIL
	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	Limiter le nombre de tentatives d'accès à un compte
Gérer les habilitations	Définir des profils d'habilitation
	Supprimer les permissions d'accès obsolètes
	Réaliser une revue annuelle des habilitations
Tracer les accès et	Prévoir un système de journalisation

Catégories	Mesures
gérer les incidents	Informer les utilisateurs de la mise en place du système de journalisation
	Protéger les équipements de journalisation et les informations journalisées
	Prévoir les procédures pour les notifications de violation de données à caractère personnel
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session
	Utiliser des antivirus régulièrement mis à jour
	Installer un « pare-feu » (*firewall*) logiciel
	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste
Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles
	Faire des sauvegardes ou des synchronisations régulières des données
	Exiger un secret pour le déverrouillage des ordiphones
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire
	Sécuriser les accès distants des appareils informatiques nomades par VPN
	Mettre en œuvre le protocole WPA2 ou WPA2-PSK, ou supérieur, pour les réseaux Wi-Fi
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	Installer sans délai les mises à jour critiques
	Assurer une disponibilité des données
Sécuriser les sites web	Utiliser le protocole TLS et vérifier sa mise en œuvre
	Vérifier qu'aucun mot de passe ou identifiant n'est encapsulé dans les URL
	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les *cookies* et autres traceurs non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr
	Prévoir des moyens de sécurité pour le convoyage des sauvegardes
	Prévoir et tester régulièrement la continuité d'activité
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
	Encadrer par un responsable de l'organisme les interventions par des tiers
	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Les relations avec les prestataires qui traitent des données au nom et pour le compte du responsable de traitement (l'organisme employeur) doivent faire l'objet d'un accord écrit. Cet accord doit contenir une ou des clauses spécifiques relatives aux obligations respectives des parties résultant du traitement des données à caractère personnel. L'accord doit notamment prévoir les conditions de restitution et de

Catégories	Mesures
	destruction des données. Il incombe au responsable de traitement de s'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.). Pour plus de précisions, vous pouvez vous reporter au guide de la sous-traitance et aux exemples des clauses de sous-traitance.
Sécuriser les échanges avec d'autres organismes	Ne pas transmettre des fichiers contenant les données à caractère personnel des usagers en clair via des messageries grand public
	Privilégier des moyens de communication autres que les messageries grand public pour communiquer des informations relatives aux personnes accompagnées à d'autres travailleurs sociaux ou organismes (p. ex. : plateformes d'échanges sécurisées, messagerie interne, etc.)
	Chiffrer les pièces sensibles à transmettre, si cette transmission utilise la messagerie électronique
	S'assurer qu'il s'agit du bon destinataire
	Assurer la confidentialité des secrets (clé de chiffrement, mot de passe, etc.) en les transmettant via un canal distinct (par exemple, envoi du fichier chiffré par courriel et transmission du secret par téléphone ou par SMS
Protéger les locaux et les bureaux physiques	Restreindre les accès aux locaux au moyen de portes verrouillées
	Installer des alarmes anti-intrusion et les vérifier périodiquement
	Ranger tous les documents papiers relatifs aux usagers dans des armoires fermées à clé
	Verrouiller la porte d'accès au bureau en cas d'absence prolongée
Encadrer les développements informatiques	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux
	Encadrer de manière stricte les zones de commentaires libres
	Tester sur des données fictives ou anonymisées
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnus
	Conserver les secrets et les clés cryptographiques de manière sécurisée
Sécuriser les mots de passe des usagers	Utiliser un gestionnaire de mots de passe ou un carnet stocké dans un coffre-fort pour enregistrer les mots de passe des usagers accompagnés dans le cadre de l'accompagnement numérique

Pour ce faire, le responsable de traitement pourra utilement se référer au Guide de la sécurité des données personnelles.

Attention :

En cas d'hébergement des données de santé à caractère personnel réalisé pour le compte des organismes assurant le suivi social ou médico-social par un prestataire informatique, celui-ci doit être agréé ou certifié pour l'hébergement, le stockage, la conservation de données de santé, conformément aux dispositions de l'article L. 1111-8 du code de la santé publique.

11. Analyse d'impact relative à la protection des données (AIPD)

Les traitements ayant pour finalité l'accompagnement social et médico-social des personnes figurant dans la liste des types d'opérations de traitement pour lesquelles une AIPD est requise, doivent systématiquement donner lieu à la réalisation préalable d'une AIPD.

Types d'opérations de traitement	Exemples
Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes	- Traitement portant sur les dossiers des résidents pris en charge par un centre communal d'action sociale (CCAS) ou par un établissement d'hébergement pour personnes âgées dépendantes (EPHAD).
Traitements ayant pour finalité l'accompagnement social et/ou médico-social des personnes	- Traitement mis en œuvre par un établissement ou une association dans le cadre de la prise en charge de personnes en insertion ou réinsertion sociale et professionnelle ; - traitement mis en œuvre par les MDPH dans le cadre de l'accueil, l'hébergement, l'accompagnement et le suivi de ces personnes ; - traitement mis en œuvre par un centre communal d'action sociale dans le cadre du suivi de personnes atteintes de pathologies chroniques invalidantes en situation de fragilité sociale.

Ce référentiel constitue une aide à la réalisation d'une AIPD. Celle-ci repose, à cet égard, sur deux piliers :

- les principes et droits fondamentaux fixés notamment par le RGPD et la loi « Informatique et Libertés » et devant être respectés quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
- la gestion des risques sur la vie privée qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données.

Pour réaliser une étude d'impact, le responsable de traitement pourra également s'appuyer sur :
- les principes contenus dans ce référentiel ;
- ainsi que sur les outils méthodologiques proposés par la CNIL sur son site web.

Si l'organisme en a désigné, le DPD/DPO devra être consulté.

Conformément à l'article 36 du RGPD, le responsable de traitement doit consulter la CNIL préalablement à la mise en œuvre du traitement si l'analyse d'impact indique qu'il ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable.