Référentiel social : un outil pour accompagner les acteurs du secteur social dans leur mise en conformité RGPD

La CNIL a publié la version définitive du référentiel le 24 mars 2021 à la suite de la consultation publique ouverte du 12 octobre 2020 au 1er décembre 2020 à laquelle la Fédération a apporté une contribution compilant les remontées faites par les membres du réseau. Le référentiel a pour objet l'encadrement des traitements de données personnelles spécifiques au secteur social et médico-social. **Ce référentiel ne vise pas à encadrer les traitements de données personnelles liés à la gestion interne de chaque structure (ressources humaines, comptabilité …).**

La production de référentiels intervient à la suite de l'abolition des démarches déclaratives issue du Règlement Général sur la protection des données[1] (RGPD) entré en vigueur le 25 mai 2018 dont l'application est obligatoire. Avant son entrée en vigueur, la CNIL avait mis en place un système d'Autorisations Uniques (AU) dont trois étaient dédiées au secteur social notamment l'AU-48[2], à laquelle la fédération avait été associée. Dans ce contexte, le référentiel, dont l'application n'est pas obligatoire, constitue un précieux outil développé par la CNIL afin de guider les structures dans leur mise en conformité dont les apports majeurs figurent ci-après. De la même manière que pour l'AU-48, la Fédération a été associée à un Groupe de Travail initié par la CNIL (GT CNIL) pour effectuer des remontées du réseau et participer à l'élaboration d'éventuels nouveaux outils.

- **Les traitements de données personnelles et acteurs concernés par le référentiel social**

Le présent référentiel a un périmètre d'application assez large puisqu'il vise : *« 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 […]* ***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.) ».***

S'agissant des organismes concernés, le référentiel prévoit une liste non exhaustive notamment 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 et les établissements sociaux et médico-sociaux[3]. A ce titre, le référentiel englobe largement les acteurs du secteur de l'action sociale puisque sont notamment visés :

- les centres communaux d'action sociale ;
- les structures relevant du dispositif de l'AHI comme celles gérant par exemple des SIAO, des centres d'accueil de jour, des CHRS ou des foyers de jeunes travailleurs ;
- les structures assurant un service d'insertion par l'activité économique (SIAE) (ex : Entreprise d'insertion, Ateliers et chantiers d'insertion) ;
- les structures accompagnant des publics spécifiques comme les personnes sous mains de justice, femmes victimes de violence, familles en difficulté et les demandeurs d'asile/réfugiés (ex : PADA, CADA, HUDA).

- **Finalités poursuivies et bases légales citées dans le référentiel**

Le référentiel précise également les finalités, c'est-à-dire les objectifs, pour lesquelles un traitement de données

[1] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

[2] CNIL, 12 mai 2016, Délibération n° 2016-095 du 14 avril 2016 portant autorisation unique de traitements de données à caractère personnel mis en œuvre dans le cadre de l'accueil, l'orientation, l'accompagnement et le suivi social des personnes (AU-048)

[3] Le Référentiel renvoie à la définition prévue à l'article L. 312-1 du code de l'action sociale et des familles (CASF)

l'Europe s'engage en France Fonds Social Européen
Fédération des acteurs de la solidarité
Ce dispositif est cofinancé par le Fonds Social Européen dans le cadre du programme opérationnel national "Emploi et Inclusion" 2014-2020
UNION EUROPÉENNE

personnelles peut être mis en œuvre. A ce titre, on peut relever les finalités de traitements de données principales ci-dessous :

- Celles relatives au fonctionnement des structures (gestion administrative financière et comptable de l'organisme (hors gestion administrative du personnel qui fait l'objet d'un autre référentiel)) ;
- Celles relatives à l'accompagnement social des personnes concernées (accompagnement social pour élaborer un projet personnalisé d'accompagnement, d'assurer le suivi des personnes dans l'accès aux droits etc.) ;
- Celles relatives à la fourniture de prestations définies dans le cadre d'un contrat conclu entre chaque personne accompagnée et l'organisme d'accueil (ex : contrat d'engagement réciproque, contrat d'hébergement..) ;
- Celles relatives aux transmissions de données comme :
  - l'échange et le 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 quand cela est autorisé par la loi et dans les conditions prévues à cet effet (ex : règles relatives aux échanges entre les professionnels de l'action sociale au sein des CHRS et des SIAO, entre les professionnels de santé et les professionnels des ESSMS);
  - la 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[4] ;
- Celles relatives à l'établissement de 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 (ex : obligation légale incombant aux structures gérant un SIAO de produire des données statistiques d'activité, de suivi et de pilotage d'accueil, d'hébergement et d'accompagnement vers l'insertion et le logement[5]).

La base légale correspond au fondement juridique qui autorise légalement la mise en place du traitement de données personnelles[6] auxquelles le référentiel en associe à chaque finalité de traitement de données personnelles précitée. Parmi les bases légales proposées, les principales retenues sont l'intérêt légitime, la mission d'intérêt public (pour les personnes morales de droit privé gérant un service public), la mise en œuvre d'une obligation légale, l'exécution d'un contrat ou le consentement. Il convient de préciser que la collecte de données sensibles est autorisée dans des cas limitatifs[7] notamment en cas de consentement des personnes concernées (point développé ci-après).

⇨ Ce point fait l'objet de discussions dans le cadre du GT CNIL car le consentement doit répondre à diverses conditions pour être valablement recueilli[8]. A cet égard, le caractère vulnérable des publics accompagnés dans le réseau a pour effet de rendre non conforme au RGPD le recueil du consentement.

- **Données personnelles pouvant être collectées et respect du principe de minimisation des données**

Conformément au principe de minimisation des données prévu par le RGPD[9], le référentiel prévoit que seules les données personnelles nécessaires à la mise en œuvre du traitement peuvent être collectées. A ce titre, les catégories de données personnelles pouvant être collectées sont listées dans le référentiel : les données d'identification, celles relatives à la vie personnelle, aux conditions de vie matérielle, au parcours professionnel et à la formation dans le

[4] L'arrêté du 28 décembre 2016 (NOR : AFSA1611822A) prévoit un modèle de formulaire pour mettre en œuvre la remontée de dysfonctionnements
[5] Article L. 345-2-4 du CASF
[6] L'article 6 du RGPD prévoit 6 bases légales
[7] Cas limitatifs prévus à l'article 9 du RGPD
[8] Les conditions sont prévues par l'article 7 du RGPD dont l'interprétation a été précisée par les lignes directrices du « Groupe 29 » étant « l'ancêtre » du Comité Européen pour la Protection des données (CEPD) qui est une institution regroupant les autorités de régulation pour la protection des données des Etats Membres de l'Union Européenne. Ces lignes directrices sont accessibles via le lien suivant : https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf
[9] Article 5.c du RGPD

cadre de l'insertion professionnelle des personnes. En outre, les modalités de collecte du NIR, des données relatives aux condamnations pénales et aux infractions et des données sensibles sont indiquées.
Concernant l'interdiction de principe de collecte de données sensibles[10] – comme les données personnelles relatives notamment à la santé, à l'orientation sexuelle - le référentiel rappelle que la collecte de telles données est possible que si l'une des dérogations prévues par le RGPD s'applique dont celles principales figurent ci-après.
Ainsi, il est possible de collecter ou d'utiliser des données sensibles : si la personne concernée a donné son consentement exprès, si les informations sont manifestement rendues publiques par la personne concernée , si cela est nécessaire à la sauvegarde de la vie humaine, si ces données sont nécessaires dans un but médical ou pour la recherche dans le domaine de la santé, si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL.
A ce titre, pour les données de santé, le référentiel propose de recueillir le consentement de la personne concernée conformément aux règles du RGPD dans le cadre de l'accompagnement social ; ce qui comporte certaines limites (cf. point développé pour les bases légales).

Quant aux données relatives aux condamnations pénales et aux infractions, le référentiel rappelle que la collecte est possible uniquement lorsque cela est autorisé par la loi[11]. Tel est le cas pour les associations de défense de victime agréée par le Ministère de la Justice, les associations d'aide à la réinsertion des personnes placées sous-main de justice, ou pour certains établissements sociaux[12].

- **Interlocuteurs du responsable de traitements et destinataires des données**

Le référentiel préconise de rendre accessible les données uniquement aux personnes habilitées à en connaitre au regard de leurs attributions ; ce qui concerne une multitude d'acteurs.

En premier lieu, **le responsable de traitement** – la structure qui détermine les moyens et les finalités du traitement de données personnelles – devra gérer les habilitations d'accès aux données afin que seules les personnes habilitées en interne au regard de leurs missions et de leurs attributions y accèdent. Par exemple, dans le cadre de l'accompagnement social de personnes en difficulté, la structure doit veiller à ce que les membres de l'équipe accèdent exclusivement aux données des personnes qu'ils accompagnent (et non à celles qu'ils n'accompagnent pas).

En second lieu, le responsable de traitement devra s'assurer de la conformité des demandes de transmission de données faites par **les destinataires des données** qui correspondent à tout organisme qui reçoit la communication des données (ex : organismes instructeurs et payeurs de prestations sociales). La conformité de la demande devra être évaluée en prenant en compte la finalité de la transmission (impliquant d'évaluer sa pertinence et sa légitimité) et des données demandées (impliquant de vérifier si elles sont adéquates, pertinentes et nécessaires au vu de la finalité de la transmission).
En cas de telles demandes, cela implique que le responsable de traitement doit vérifier notamment avant toute transmission de données si cette demande est autorisée par un texte légal, la base légale fondant la transmission, la conformité de la finalité de la transmission et si le périmètre des données demandées se limite à celles nécessaires au regard de la finalité de la transmission et les mesures de sécurité prévues pour l'envoi des données et leur traitement. Si la demande ne précise pas ces éléments, il faut les demander à la personne à l'origine de la demande et examiner, ensuite, sa conformité à la lumière des éléments ultérieurs adressés. Par ailleurs, il convient de noter qu'un guide relatif aux tiers autorisés a été publié et comporte des recommandations pratiques très utiles. **Les tiers autorisés**, catégorie particulière de destinataires, sont des autorités et organismes (publics le plus souvent) disposant, en vertu

[10] Prévue à l'article 9 du RGPD
[11] Article 46 de la loi Informatique et Libertés et article 76 du décret n°2019-536 du 29 mai 2019
[12] Notamment les établissements et services intervenant dans le domaine de la protection judiciaire de la jeunesse ou gérant des lieux d'accueil et de vie

de l'intérêt public qui s'attache à l'accomplissement de leur mission, du pouvoir de solliciter l'obtention de données à caractère personnel issues de fichiers détenus par des personnes ou organismes publics et privés.

⇨ Dans le cadre du GT CNIL, des travaux sont consacrés aux échanges de données incluant la gestion des demandes de tiers autorisés et notamment aux textes qui fondent leur droit de communication de données.

En troisième lieu, le référentiel rappelle les règles applicables d'une part, dans le cadre de la relation entre le responsable de traitement et **le sous-traitant** et rappelle la publication d'un guide du sous-traitant qui prévoit notamment des outils afin d'assurer la mise en conformité.

- **Durée de conservation des données**

La conservation des données personnelles doit être d'une durée nécessaire de telle sorte que les données doivent être supprimées ou restituées une fois cette durée passée[13]. La CNIL a rédigé un guide pratique relatif à la durée de conservation des données précisant le principe de limitation de la conservation des données et ses implications
Le référentiel propose une durée de conservation des données personnelles générale s'appliquant à l'ensemble des finalités prévues s'élevant à deux ans à compter du dernier contact avec la personne accompagnée en « base active » (c'est-à-dire à usage immédiat). Le référentiel précise que cela s'applique sauf si un texte règlementaire ou légal prévoit une autre durée (ex : durée de CDDI conclu entre une personne sans emploi et un Atelier et chantier d'insertion peut aller, exceptionnellement, jusqu'à 60 mois[14]). Il est possible de conserver les données plus longtemps en archivage intermédiaire si cela est nécessaire (ex : archivage intermédiaire au-delà de la durée précitée en base active pour respecter une obligation comptable, sociale ou fiscale ou se ménager une preuve en cas de contentieux).

⇨ Cette durée générale préconisée de deux ans n'est pas adaptée aux traitements de données mis en œuvre par les membres du réseau pour assurer leur mission et ne semblent pas conformes aux réalités de terrain. Ce point fait l'objet de discussions dans le cadre du GT CNIL.

- **Information et droits des personnes**

Le référentiel rappelle l'obligation d'informer les personnes accompagnées au sujet des traitements de ses données personnelles mis en œuvre par le responsable de traitement[15]. De nombreux éléments doivent figurer dans cette information devant être claire et compréhensible dont la forme écrite est vivement recommandée[16]. Les modalités d'information des publics accompagnés à prévoir sont essentielles pour favoriser leur bonne compréhension. A cet égard, le référentiel préconise non seulement une information écrite et une autre orale et de favoriser le recours à la méthode Facile à Lire Facile à Comprendre (FALC).

⇨ C'est pourquoi, dans le GT CNIL, des travaux sont initiés (élaboration de mention type d'information notamment).

Concernant les droits des personnes concernées[17], le référentiel rappelle sa typologie (notamment le droit d'accès, droit de rectification et d'opposition au traitement) et rappelle les modalités de refus de donner suite à une demande d'exercice du droit d'opposition.

[13] Principe de limitation de la conservation des données prévu à l'article 5.e du RGPD
[14] Article L5132-15-1 du code de travail prévoit la possibilité de prolonger le CDDI au-delà de la durée de initiale de 24 mois pour les salariés rencontrant *« des difficultés particulièrement importantes dont l'absence de prise en charge ferait obstacle à leur insertion professionnelle »*
[15] Règles relatives à l'information des personnes énoncées aux articles 13 et 14 du RGPD
[16] Le responsable de traitement ayant l'obligation de conserver une preuve de la mise en œuvre de cette information conformément au RGPD
[17] Les droits des personnes sont prévus aux articles 12 à 23 du RGPD

- **Mesures de sécurité**

Le responsable de traitement doit assurer la sécurité des traitements de données personnelles[18]. Un ensemble de mesures techniques et organisationnelles non exhaustives sont préconisées dans le référentiel (ex : gérer les habilitations pour assurer la confidentialité des données, sécuriser les postes informatiques internes). Pour plus d'informations, un guide relatif à la sécurité des données personnelles a été publiée par la CNIL : Guide sécurité des données personnelles (cnil.fr).

- **Outils et bonnes pratiques principales pour assurer une mise en conformité au RGPD optimale**

  - **Recommandations pour être accompagné par un DPO**

Le référentiel recommande, en filigrane, de désigner un Délégué à la Protection des données (DPO), qui dispose d'une expertise en matière de protection des données, ayant pour mission de mettre en œuvre la conformité au RGPD au sein de la structure du responsable de traitement. **Ce DPO peut être une personne en interne ou en externe**. Dans ce dernier cas, il peut être **mutualisé** avec d'autres structures (pour plus d'informations : https://www.cnil.fr/fr/definition/delegue-protection-donnees).

  - **Analyse d'impact relative à la protection des données (AIPD) obligatoire**

Le référentiel rappelle que les structures, responsables de traitements, mettant en œuvre des traitements ayant pour finalité l'accompagnement social et médico-social de personnes doivent mettent en œuvre une AIPD de manière obligatoire conformément à une délibération de la CNIL[19]. C'est un outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée, lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Cela implique de la réaliser préalablement à toute mise en œuvre de traitements. Pour les structures ne l'ayant pas réalisée, il est recommandé de la déployer dès que possible. A cet effet, la CNIL a développé divers outils permettant d'aider les responsables de traitement à la réaliser, en consultation avec le DPO, en s'aidant d'une part du référentiel et des outils mis à disposition par la CNIL (liens vers les outils méthodologiques : https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd).

  - **Registres de traitements obligatoires**

L'obligation de tenir un registre de traitements découlant du RGPD doit être mise en œuvre par les structures d'une part pour leurs activités de responsables de traitements et pour leurs activités de sous-traitance de données. Ces outils sont soumis à un formalisme précis imposés par le RGPD dont la CNIL a publié un modèle pour les activités du responsable de traitements.

**

En conclusion, le référentiel est l'outil de référence pour guider les acteurs du secteur social dans leur mise en conformité. Néanmoins, des points particuliers demeurent à être clarifiés notamment s'agissant des modalités de recueil du consentement et d'information des personnes concernées, de la détermination des durées de conservation dans le secteur social, sur les modalités de complétude de registres et d'AIPD et du cadre des échanges de données (notamment avec les tiers autorisés). Ces axes correspondent aux thèmes de travail fixés dans le cadre du GT CNIL

[18] Article 34 du RGPD

[19] Délibération n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise

auquel la Fédération participe. La Fédération va donc contribuer à remonter les difficultés éprouvées au sein du réseau en vue de favoriser des évolutions de ce cadre et d'initier la création d'outils complémentaires du type FAQ, modèles de mentions d'informations.

Si vous souhaitez nous adresser vos remontées, n'hésitez pas à contacter Sarra Cheklab (chargée de mission RGPD, inclusion numérique et accès aux droits) : sarra.cheklab@federationsolidarite.org

l'Europe s'engage en France
Fonds Social Européen
Fédération des acteurs de la solidarité
UNION EUROPÉENNE
Ce dispositif est cofinancé par le Fonds Social Européen dans le cadre du programme opérationnel national "Emploi et Inclusion" 2014-2020