CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

AU 47

Accompagnement et suivi social et médico-social des personnes handicapées et des personnes âgées

Suite à l'entrée en application du RGPD, les normes adoptées par la CNIL n'ont plus de valeur juridique depuis le 25 mai 2018.

Dans l'attente de la production de référentiels RGPD, les responsables de traitement peuvent s'en inspirer pour orienter leurs premières actions de conformité.

La CNIL attire toutefois l'attention sur la nécessité de veiller au respect des nouvelles règles.

Accompagnement et suivi social et médico-social des personnes handicapées et des personnes âgées

(Déclaration N° 47)

Suite à l'entrée en application du RGPD, les autorisations uniques adoptées par la CNIL n'ont plus de valeur juridique à compter du 25 mai 2018. Dans l'attente de la production de référentiels RGPD, la CNIL a décidé de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mise en conformité.

L'autorisation unique n° AU-047 concerne les traitements mis en œuvre par les établissements, services ou organismes intervenant auprès des personnes âgées ou des personnes handicapées aux fins d'assurer un accompagnement et un suivi personnalisé tout au long de leurs parcours, et un partage sécurisé des données entre les acteurs sociaux, médicaux et paramédicaux.

Ne sont pas couverts par cette autorisation unique, les traitements comportant le numéro de sécurité sociale qui sont mis en œuvre pour le compte de l'État, d'une personne morale de droit public ou de droit privé gérant une mission de service public ainsi que les traitements ayant pour objectif le suivi de la procédure de signalement des situations de maltraitance.

Toutes les données figurant dans l'autorisation unique n'ont pas vocation à être systématiquement collectées. Seules les données strictement nécessaires à la mise en œuvre du suivi social et médico-social de la personne concernée, ou de son représentant légal, peuvent faire l'objet d'un traitement.

TEXTE OFFICIEL

Délibération n° 2016-094 du 14 avril 2016 portant autorisation unique de traitements de données à caractère personnel mis en œuvre dans le cadre de l'accueil, l'hébergement, l'accompagnement et le suivi des personnes handicapées et des personnes âgées.

Responsables de traitement concernés

Services, établissements ou organismes publics et privés.

Objectif(s) poursuivi(s) par le traitement (finalités)

- gestion administrative des personnes concernées ;
- saisie des problématiques identifiées dans le cadre de l'évaluation sociale et médico-sociale des personnes en vue de leur garantir un accompagnement adapté et, le cas échéant, les orienter vers les structures compétentes susceptibles de les prendre en charge ;
- élaboration et suivi du projet personnalisé d'accompagnement des personnes ;
- échange et partage d'informations entre les intervenants sociaux, médicaux et paramédicaux des informations strictement nécessaires permettant de garantir la coordination et la continuité de l'accompagnement et du suivi des personnes ;
- gestion des demandes d'attribution de places en établissement ou service, médicalisé ou non, et des demandes d'aides à domicile ;
- gestion et tenue des dossiers individuels de soins dans le cadre du suivi médical des personnes, comprenant la gestion des remboursements de frais médicaux ;
- gestion et suivi des activités individuelles ou collectives des personnes ;
- organisation et suivi des parcours d'insertion et/ou d'intégration scolaire, sociale et professionnelle pour les personnes handicapées ;
- accompagnement et suivi des personnes dans l'accès aux droits, y compris les droits relatifs à la fin de vie ;
- contrôle d'effectivité du plan d'aide à partir des besoins, du montant des prestations, de leur réalisation et de leur évaluation ;
- gestion financière et comptable de l'établissement, du service ou de l'organisme ;
- établissement de statistiques, d'études internes et d'enquêtes de satisfaction aux fins d'évaluation des activités, de la qualité des prestations et des besoins à couvrir.

Utilisation(s) exclue(s) du champ de la norme

Le suivi de la procédure de signalement de situations de maltraitance.

Données personnelles concernées

- les données d'identification des bénéficiaires de l'accompagnement et du suivi social et médico-social et, le cas échéant, de leurs représentants légaux : nom, prénom, sexe, adresse, courriel, numéro de téléphone, date et lieu de naissance, photographie, numéro d'identification de rattachement à un organisme (numéro d'adhérent ou allocataire) et numéro de sécurité sociale (uniquement dans le cadre d'échanges avec les professionnels de santé, les organismes de sécurité sociale, de prévoyance ou des fournisseurs de matériel ou produits médicaux) ;
- 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 ;
- des informations relatives à la vie personnelle du bénéficiaire : situation et composition familiale du foyer, habitudes de vie nécessaires à l'organisation de la vie quotidienne, centres d'intérêt, langue parlée dans la mesure où cette information est indispensable pour mentionner le besoin de traducteurs ;
- la nature de la mesure de protection juridique, et le cas échéant les coordonnées du mandataire ;

- le parcours professionnel et de formation dans le cadre de l'aide à l'insertion professionnelle des personnes handicapées (scolarité, situation au regard de l'emploi, de la formation et de la qualification) ;
- la situation professionnelle antérieure des personnes âgées lorsque cette information est nécessaire à un accompagnement et un suivi adapté à leurs besoins ;
- les conditions de vie matérielles :
    - situation financière (ressources, charges, crédits, dettes) ;
    - prestations et avantages sociaux perçus (nature, montant, quotient familial, numéro 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.
- la couverture sociale : organismes de rattachement et régimes d'affiliation, droits ouverts ;
- les coordonnées bancaires dans la mesure où cette information est nécessaire au versement d'une prestation ;
- la santé à des fins d'administration de soins, comprenant les informations relatives au handicap. Ces données peuvent être collectées à d'autres fins, sous réserve du consentement exprès des personnes concernées ou de leurs représentants légaux, d'une part, et d'être strictement nécessaires au suivi social et médico-social, d'autre part ;
- la vie sexuelle (orientation sexuelle et conduite sexuelle), sous réserve d'être directement collectées auprès des personnes concernées, après le recueil de leur consentement exprès ou celui de leurs représentants légaux, et d'être strictement nécessaires pour organiser des actions de prévention et assurer une éducation sexuelle adaptée dans le cadre de la prise en charge des personnes handicapées, et, le cas échéant, pour faire intervenir un professionnel de santé si la personne concernée est confrontée à des risques particuliers au regard de sa sexualité ;
- les opinions religieuses sous réserve d'être collectées auprès des personnes concernées ou de leurs représentants légaux, après le recueil d'un consentement exprès et d'être strictement nécessaires à une prise en charge adaptée et respectueuse des convictions des personnes concernées ;
- l'évaluation sociale et médico-sociale des personnes concernées (difficultés et appréciations sur les difficultés rencontrées, évaluation de la situation des personnes afin de repérer une aggravation d'une perte d'autonomie) ;
- le type d'accompagnement des personnes et les actions mises en œuvre (domaines d'intervention, historique des mesures d'accompagnement, objectifs, parcours, actions d'insertion prévues, entretien et suivi) ;
- mention de l'existence d'une situation de maltraitance, afin d'adapter l'accompagnement de la personne concernée. En revanche, sont exclues les données relatives à une éventuelle procédure en cours ou à l'existence d'une enquête pénale ;
- les directives anticipées, et le cas échéant le nom et la qualité de la personne de confiance ;
- les données d'identification des personnes concourant à la prise en charge sociale et médico-sociale ainsi qu'à l'entourage susceptible d'être contacté (aidants professionnels ou familiaux, médecin traitant, médecins experts, personne de confiance) : nom, prénom, qualité, organisme d'appartenance, numéro de téléphone, adresse, courriel, téléphone.

Durée de conservation des données

Les données collectées et traitées pour les besoins du suivi social ou médico-social ne peuvent être conservées dans la base active au-delà de deux ans à compter du dernier contact avec la personne ayant fait l'objet de ce suivi, sauf dispositions législatives ou réglementaires contraires. Ces données doivent être supprimées sans délai en cas de décès de la personne concernée.

Lorsqu'il existe un recours contre un tiers ou un contentieux, les données peuvent être conservées jusqu'à l'intervention de la décision définitive.

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.

Les justificatifs recueillis, y compris sous format papier, qui n'ont plus d'utilité, soit parce qu'ils sont trop anciens pour justifier de la situation de l'usager, soit parce que le dossier pour lequel ils ont été demandés est constitué, doivent être détruits.

Destinataires des données

Dans les limites de leurs attributions légales, et chacun pour ce qui le concerne, peuvent accéder aux données de la présente autorisation unique :

- le personnel au sein de chaque établissement, service ou organisme concourant à la prise en charge, à l'accompagnement et au suivi social et médico-social des personnes ;
- les professionnels et tout membre du personnel de l'établissement, du service ou organisme externe, participant à la prise en charge, à l'accompagnement et au suivi de la personne, et toute autre personne en relation, de par ses activités, avec ces établissements ou organismes externes, dans la limite de leurs attributions respectives et des règles encadrant le partage et l'échange d'informations ;
- 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 ;
- des 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 relatives aux personnes visées par la présente autorisation unique.

Toute demande d'informations en vue d'une étude statistique fera l'objet d'une transmission de données préalablement anonymisées.

Information des personnes et respect des droits « informatique et libertes »

Le responsable du traitement doit informer les personnes concernées par le ou les traitements mis en œuvre par tout moyen approprié, dans un langage compréhensible et selon des modalités appropriées et adaptées à leur état.

L'information doit notamment porter sur l'identité du responsable de traitement, la finalité poursuivie par le traitement, les destinataires des données et les droits des personnes (droits d'opposition pour motifs légitimes, d'accès et de rectification).

Les personnes sont également informées du caractère obligatoire ou facultatif des réponses, ainsi que des conséquences éventuelles, à leur égard, d'un défaut de réponse ou de l'exercice de leur droit d'opposition.

Cette information doit notamment figurer sur les formulaires de collecte destinés aux personnes auprès desquelles les données sont collectées.

Les droits d'opposition, pour motifs légitimes, d'accès et de rectification s'exercent directement auprès du ou des services que le responsable de traitement doit impérativement désigner.

Sécurité et confidentialité

Le responsable de traitement doit prendre toutes les précautions utiles au regard des risques présentés par le traitement pour préserver la sécurité des données à caractère personnel. Il doit, notamment s'assurer que :

- toute transmission d'information via un canal de communication non sécurisé, par exemple Internet, s'accompagne de mesures adéquates permettant de garantir la confidentialité des données échangées, telles qu'un chiffrement des données ;
- les personnes habilitées disposant d'un accès aux données doivent s'authentifier avant tout accès à des données à caractère personnel, au moyen d'un identifiant et d'un mot de passe personnels respectant les recommandations de la CNIL, ou par tout autre moyen d'authentification garantissant au moins le même niveau de sécurité ;
- un mécanisme de gestion des habilitations est mis en œuvre et régulièrement mis à jour pour garantir que les personnes habilitées n'ont accès qu'aux seules données effectivement nécessaires à la réalisation de leurs missions. Le responsable de traitement doit définir et formaliser une procédure permettant de garantir la bonne mise à jour des habilitations ;
- des mécanismes de traitement automatique garantissent que les données à caractère personnel seront systématiquement supprimées, à l'issue de leur durée de conservation, ou feront l'objet d'une procédure d'anonymisation rendant impossible toute identification ultérieure des personnes concernées ;
- les accès à l'application font l'objet d'une traçabilité afin de permettre la détection d'éventuelles tentatives d'accès frauduleux ou illégitimes. Les accès aux données considérées comme sensibles, au regard de la loi du 6 janvier 1978 modifiée, doivent quant à eux être spécifiquement tracés en incluant un horodatage, l'identifiant de l'utilisateur, ainsi que l'identification des données concernées, et ceci pour les accès en consultation, modification ou suppression. Les données de journalisation doivent être conservées pendant une durée de six mois glissants à compter de leur enregistrement, puis détruites ;
- l'externalisation de l'hébergement de données de santé à caractère personnel soit réalisée dans les conditions prévues dans le code de la santé publique.

Concernant les mécanismes d'anonymisation, il conviendra de s'assurer que les statistiques produites ne permettent aucune identification, même indirecte, des personnes concernées.

L'usage d'outils ou de logiciels développés par des tiers dans le cadre de la mise en œuvre d'un traitement de données à caractère personnel reste sous la responsabilité du responsable de traitement, qui doit notamment vérifier que ces outils ou logiciels respectent les obligations que la loi met à sa charge.

Enfin, le responsable de traitement conserve la responsabilité des données à caractère personnel communiquées ou gérées par ses sous-traitants. Le contrat établi entre les parties doit mentionner les obligations incombant au sous-traitant en matière de préservation de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instructions du responsable de traitement.

Transferts des donnes hors de l'union européenne

Un transfert de données à caractère personnel à destination d'un pays tiers à l'Espace économique européen peut être effectué lorsque l'une des conditions suivantes est réunie :

- le transfert s'effectue à destination d'un pays reconnu par une décision de la Commission européenne comme assurant un niveau de protection suffisant ;
- le traitement garantit un niveau suffisant de protection de la vie privée, ainsi que les droits et libertés fondamentaux des personnes, par la mise en œuvre de clauses contractuelles rédigées sur les modèles de clauses élaborés par la Commission européenne relatives aux transferts de données, d'une part, ou par l'adoption de règles internes d'entreprise (« Binding Corporate Rules » ou BCR) adoptées par le responsable de traitement et reconnues par la Commission nationale de l'informatique et des libertés et les autorités de protection des données personnelles compétentes comme offrant un cadre juridique satisfaisant pour effectuer des transferts de données en dehors de l'Union européenne, d'autre part ;
- le transfert est justifié par le respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice.

Le recours aux exceptions n'est possible que pour les transferts dont le champ d'application est limité à des cas ponctuels et exceptionnels. Les transferts répétitifs, massifs ou structurels de données doivent quant à eux faire l'objet d'un encadrement juridique spécifique, par l'intermédiaire de BCR ou de clauses contractuelles types.

Le responsable de traitement s'engage, sur simple demande d'une personne concernée, à apporter une information complète sur la finalité du transfert, les données transférées, les destinataires exacts des informations et les moyens mis en œuvre pour encadrer ce transfert.