Commission nationale de l'informatique et des libertés

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 (AU-047)

NOR : *CNIL1611475X*

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code de l'action sociale et des familles ;

Vu le code de procédure pénale ;

Vu le code de la santé publique, notamment son article L. 1111-4 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 25-II ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu Mme Laurence DUMONT, commissaire, en son rapport, et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Dans la sphère sociale et médico-sociale, les établissements, services ou organismes intervenant auprès des personnes âgées ou des personnes handicapées assurent l'accueil, médicalisé ou non, des personnes, à titre permanent, temporaire ou selon un mode séquentiel, avec ou sans hébergement, ainsi que leur accompagnement et suivi en milieu de vie ordinaire, en accueil familial ou dans une structure de prise en charge.

Une prise en charge coordonnée et adaptée des personnes nécessite une évaluation continue de leurs besoins et de leurs difficultés, afin d'établir un accompagnement et un suivi personnalisé tout au long de leur parcours, et un partage sécurisé des données entre les acteurs sociaux, médicaux et paramédicaux.

Dans le cadre de leurs missions, les structures prenant en charge les personnes âgées ou les personnes handicapées sont amenées à mettre en œuvre des traitements comportant des données sensibles telles que des données de santé ou des appréciations sur les difficultés sociales des personnes. Par ailleurs, des échanges avec des organismes de sécurité sociale peuvent être nécessaires et, à ce titre, impliquent l'utilisation du numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (numéro de sécurité sociale ou NIR).

Dès lors, de tels traitements relèvent des articles 8 (IV), 25 (I, 1°), 25 (I, 6°) et 25 (I, 7°) de la loi du 6 janvier 1978 susvisée et doivent, à ce titre, être autorisés par la CNIL.

Toutefois, afin d'alléger les formalités que doivent accomplir les professionnels, la commission a souhaité faire application des dispositions de l'article 25 (II) de la loi du 6 janvier 1978 modifiée, en vertu desquelles elle peut autoriser par une décision unique une catégorie de traitements qui répondent aux mêmes finalités, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires.

Les traitements, qu'ils soient automatisés ou non, portant sur des données à caractère personnel ainsi que les seuls traitements automatisés comportant des données relatives aux appréciations sur les difficultés sociales mis en œuvre par les établissements, services ou organismes, aux fins d'accompagnement et de suivi social et médico-social des personnes âgées ou des personnes handicapées, sont de ceux qui peuvent relever de cette définition.

Les responsables de traitement qui adressent à la commission une déclaration comportant un engagement de conformité pour les traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à les mettre en œuvre.

Tout traitement de données à caractère personnel qui excède le cadre ou les exigences définis par la présente autorisation unique doit en revanche faire l'objet d'une formalité spécifique auprès de la commission.

Art. 1er. – *Champ d'application.*

Seuls peuvent faire l'objet d'un engagement de conformité en référence à la présente autorisation unique les traitements mis en œuvre par les organismes assurant l'accueil, la prise en charge, l'accompagnement et le suivi social et médico-social des personnes âgées ou des personnes handicapées et de leurs familles.

Sont exclus du champ de cette autorisation unique :

– les traitements mis en œuvre pour le compte de l'Etat, d'une personne morale de droit public ou de droit privé gérant une mission de service public, dès lors qu'ils comportent le NIR. De tels traitements doivent être décidés par un acte réglementaire, conformément à l'article 27 de la loi ;
– les traitements ayant pour finalité le suivi de la procédure de signalement de situations de maltraitance.

Art. 2. – *Sur les finalités des traitements.*

Les traitements mis en œuvre par les professionnels intervenant auprès des personnes âgées ou des personnes handicapées ainsi que de leur famille visent à permettre :

– la gestion administrative des personnes concernées ;
– la 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 ;
– l'élaboration et le suivi du projet personnalisé d'accompagnement des personnes, conformément aux dispositions des articles L. 311-3 et L. 311-4 du code de l'action sociale et des familles ;
– l'échange et le 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 ;
– la gestion des demandes d'attribution de places en établissement ou service, médicalisé ou non, et des demandes d'aides à domicile ;
– la gestion et la tenue des dossiers individuels de soins dans le cadre du suivi médical des personnes, comprenant la gestion des remboursements de frais médicaux ;
– la gestion et le suivi des activités individuelles ou collectives des personnes ;
– l'organisation et le suivi des parcours d'insertion et/ou d'intégration scolaire, sociale et professionnelle pour les personnes handicapées ;
– l'accompagnement et le suivi des personnes dans l'accès aux droits, y compris les droits relatifs à la fin de vie ;
– le contrôle d'effectivité du plan d'aide à partir des besoins, du montant des prestations, de leur réalisation et de leur évaluation ;
– la gestion financière et comptable de l'établissement, du service ou de l'organisme ;
– l'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.

Art. 3. – *Sur les catégories de données collectées et traitées.*

A titre liminaire, la commission rappelle que des données à caractère personnel ne peuvent être collectées que si elles sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie.

L'ensemble des données suivantes n'ont pas vocation à être systématiquement recueillies. 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. Dès lors, le responsable de traitement doit être en mesure de justifier du caractère nécessaire et proportionné des données à caractère personnel pour les besoins du travail poursuivi.

Sous ces réserves, les établissements, services ou organismes intervenant auprès des personnes âgées ou des personnes handicapées ainsi qu'auprès de leurs familles peuvent, pour atteindre les finalités visées à l'article 2 de la présente autorisation unique, collecter et traiter des données relatives :

– à l'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), numéro de sécurité sociale ;

  S'agissant du numéro de sécurité sociale, il ne peut être enregistré dans le traitement que 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 ;

  Peuvent également 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 ;
– à la vie personnelle : 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 ;
– à la nature de la mesure de protection juridique et, le cas échéant, les coordonnées du mandataire ;
– au 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) ;
– à la situation professionnelle antérieure des personnes âgées lorsque cette information est nécessaire à un accompagnement et un suivi adapté à leurs besoins ;

- aux 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 ;
- 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 ;
- à 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 ;
- à 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 ;
- aux 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 ;
- à 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) ;
- au type d'accompagnement des personnes et aux actions mises en œuvre (domaines d'intervention, historique des mesures d'accompagnement, objectifs, parcours, actions d'insertion prévues, entretien et suivi) ;
- à 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 ;
- aux directives anticipées et, le cas échéant, le nom et la qualité de la personne de confiance ;
- à l'identification des personnes concourant à la prise en charge sociale et médico-sociale et 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.

Art. 4. – *Sur la durée de conservation des données.*

La commission rappelle que, conformément à l'article 6-5° de la loi du 6 janvier 1978 modifiée, des données à caractère personnel ne peuvent être conservées que le temps strictement nécessaire à l'accomplissement de la finalité pour laquelle elles ont été collectées.

En tout état de cause, 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.

A 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 commission n° 2005-213 du 11 octobre 2005 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.

Art. 5. – *Sur les catégories de destinataires des données.*

Compte tenu de leur caractère sensible, le partage des informations collectées doit s'entourer de garanties spécifiques.

Ainsi, 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.

Les 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 et ne peuvent 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.

La commission rappelle que les informations échangées sont protégées au titre du secret professionnel, dans les conditions prévues aux articles 226-13 et 226-14 du code pénal, sous réserve des dérogations prévues expressément par la loi et permettant le partage des informations.

En particulier, le partage d'informations doit être réalisé dans les conditions prévues aux articles L. 121-6-2 et L. 226-2-2 du code de l'action sociale et des familles et L. 1110-4 du code de la santé publique.

En tout état de cause, il revient au responsable de traitement, avant chaque transmission des données, d'opérer un tri parmi ces dernières pour s'assurer que le destinataire accède aux seules données strictement nécessaires et proportionnées au regard de la justification de la transmission.

La commission rappelle, par ailleurs, que 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.

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.

Dans les limites de leurs attributions légales, et chacun pour ce qui le concerne, peuvent accéder aux données visées à l'article 3 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.

En tout état de cause, toute demande d'informations en vue d'une étude statistique fera l'objet d'une transmission de données préalablement anonymisées.

Art. 6. – *Sur l'information et les droits des personnes.*

Le responsable du traitement procède, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée, à l'information des 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 définis au chapitre V de la loi du 6 janvier 1978 modifiée s'exercent directement auprès du ou des services que le responsable de traitement doit impérativement désigner.

Art. 7. – *Sur les mesures de sécurité.*

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 au moment de leur collecte, durant leur transmission et leur conservation, empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès.

A cet égard, le responsable de traitement 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 soit mis en œuvre et régulièrement mis à jour pour garantir que les personnes habilitées n'aient 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 fassent 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 cela 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 à l'article L. 1111-8 du 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.

La commission rappelle que 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 du 6 janvier 1978 modifiée 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.

Art. 8. – *Sur les transferts de données.*

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 l'exception prévue par le 3° de l'article 69 de la loi du 6 janvier 1978 modifiée, à savoir le respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice.

La commission rappelle que le recours aux exceptions prévues par l'article 69 de la loi du 6 janvier 1978 modifiée 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.

Art. 9. – *Publication.*

La présente délibération sera publiée au *Journal officiel* de la République française.

Fait le 14 avril 2016.

La présidente,
I. Falque-Pierrotin