Collectif SI Médico-Social Hauts-de-France

SDC avocats
68 rue de Wambrechies
Immeuble SDC Parc de Haut-Touquet
59520 MARQUETTE-LEZ-LILLE
Tél. 03 20 78 54 80

Sandrine MINNE
Avocat spécialisé
DROIT DES NTIC
DROIT DE LA PROPRIÉTÉ INTELLECTUELLE
DROIT DES AFFAIRES
sandrine.minne@sminne-avocat.fr
www.sminne-avocat.fr

RGPD

QUOI DE NEUF ?

Rappel des principes de base :

Le Règlement Général sur la Protection des Données, entré en vigueur le 25 mai 2018, implique avant tout un devoir d'information auprès des utilisateurs concernés par le traitement de leurs données personnelles. En tant que responsable du traitement de ces données, ou bien en tant que sous-traitant, il convient de prendre les mesures nécessaires pour garantir une utilisation respectueuse de ces données, permettant la protection de la vie privée des personnes concernées, mais aussi de leurs droits à cet égard.

Pour ce faire, quelques règles fondamentales s'imposent :

Avant tout processus de traitement de données, posez-vous les bonnes questions, à savoir : est-ce réellement nécessaire dans le cadre de mon activité ? Quelles sont les données indispensables et celles qui ne le sont pas ? Est-ce bien pertinent de collecter ces données et en ai-je le droit ? Les personnes concernées ont-elles étaient correctement informées et ont-elles explicitement donné leur accord ?

Le RGPD implique une totale transparence quant à l'utilisation des données collectées. Les personnes faisant l'objet d'une collecte de données doivent pouvoir vous faire confiance.

Vous devez être en mesure de répondre, dans les meilleurs délais, aux demandes des utilisateurs concernés quant à leurs droits de consultation, de rectification, de transmission, mais également de suppression définitive de leurs données.

Votre structure doit, après avoir identifié les risques, être en mesure d'assurer un partage et une circulation encadrés des données personnelles, afin de leur assurer une protection optimale, tout au long du processus de traitement. Des mesures spécifiques doivent être prises si les données concernées sont dites sensibles (relatives à des opinions politiques, une origine raciale, une orientation sexuelle, etc).

Gardez bien à l'esprit que les mesures de sécurité doivent être adaptées en fonction des risques qui pèsent sur les personnes concernées en cas d'exploitation non consentie de leurs données personnelles. Ces mesures de sécurité, informatiques comme physiques, doivent permettre la totale sécurité de ces données à risque.

Le RGPD prévoit un certain nombre de sanctions en cas de non-respect du RGPD ou d'une violation ponctuelle constatée. Celles-ci peuvent être très importantes puisque, selon les cas, elles peuvent atteindre jusqu'à 4 % du chiffre d'affaires global de la société ou jusqu'à 20 millions d'euros, le chiffre le plus important étant retenu.

Illustrations en europe :

Non-respect du consentement: 1.200.000€ (DE)

Une assurance avait organisé une série de concours ayant pour objectif de collecter les données personnelles de prospects et clients. L'entreprise a réutilisé ces données pour faire de la publicité, initialement en s'assurant que les personnes avaient bien donné leur consentement.

Violation de données personnelles par un avocat : 2000€ (ES)

75.000€ de sanctions pour un refus de suppression de données personnelles (ES)

288.000€ de sanctions pour collecte disproportionnée de données (HU)

Conservation trop longue des données : 75.000€

10.000€ de sanctions pour un email reçu sans consentement (BE)

112.000€ de sanctions pour un hopital n'ayant pas protégé les données de

I- RGPD et médico social – piqûre de rappel

LE RGPD au cœur de l'actu plan ESMS numérique pour 2020

Tout d'abord, ce plan doit concerner toutes les structures – y compris celles du secteur social -, et, en particulier, permettre à celles qui n'ont pas encore entrepris leur transformation numérique de se lancer dedans au moyen d'apports en ingénierie et par l'incitation à la mutualisation.

Ensuite, le plan doit permettre à toutes les structures de faire un pas de plus dans les directions suivantes :

- la numérisation du parcours de l'usager au sein de la structure en assurant la convergence des projets avec le DMP et l'ENS ;
- la sécurité des données via :
  - la généralisation de la messagerie sécurisée,
  - l'hébergement certifié « Hébergement données de santé » (HDS),
  - la gestion des solutions mobiles,
  - la promotion d'une culture de la sécurité dans les organisations ;
- la gestion du cycle de vie, la conservation et l'archivage (sécurisé) des données.

Avant RGPD, la matière était régie par la norme AU47 : Accompagnement et suivi social et médico-social des personnes handicapées et des personnes âgées qui peut encore servir de référentiel :

1- Les finalités admises

- 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.

2- Les données

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 ; 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. cnil fr 4 Accompagnement et suivi social et médico-social des personnes handicapées et des personnes âgées - AU 47 • 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.

3- La documentation démontrant la conformité

Les dispositions du RGPD s'appliquent à tous les traitements de données personnelles (ex : nom, prénom, numéro de patient, etc.) que les établissements utilisent pour l'exercice de leurs activités professionnelles, que ces traitements soient sous une forme informatique ou papier (ex : dossier patient papier).

Chaque établissement doit donc :

- Disposer d'un registre des activités de traitements ;
- Assurer le respect des droits des personnes ;
- Avoir mis en place des procédures garantissant la sécurité et la confidentialité des données ;
- Disposer d'un délégué à la protection des données ;
- Avoir réalisé une analyse de l'impact du traitement des données sensibles (notamment les informations de santé)
- Avoir assuré la sécurité de ses relations contractuelles ;
- Prévoir le signalement de tout incident de sécurité.
- Les données des usagers ne peuvent être gardées indéfiniment

4- Les données que vous collectez sur les usagers doivent être conservées pour une durée déterminée.

On considère généralement que les données collectées et traitées pour les besoins du suivi social ou médico-social ne peuvent être légitimement conservées dans une base active au-delà de deux ans à compter du dernier contact avec la personne ayant fait l'objet de ce suivi. Ces données devraient par ailleurs 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 devraient être 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 recommandations de la CNIL 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.

5- Destinataires des données des usagers

Dans les limites de leurs attributions légales, et chacun pour ce qui le concerne, peuvent légitimement accéder aux données personnelles des usagers :

- 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.

6- Sécurité et confidentialité de l'informatisation

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

7- Les usagers doivent être informés du traitement de leurs données mais vous n'avez pas à recueillir leur consentement

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.

8- Points de vigilance

Attention à la vidéosurveillance

Attention aux données des salariés et au rappel de leurs obligations : lien avec les contrats de travail et la charte informatique.

II- Les données de santé

1- La hiérarchie des données

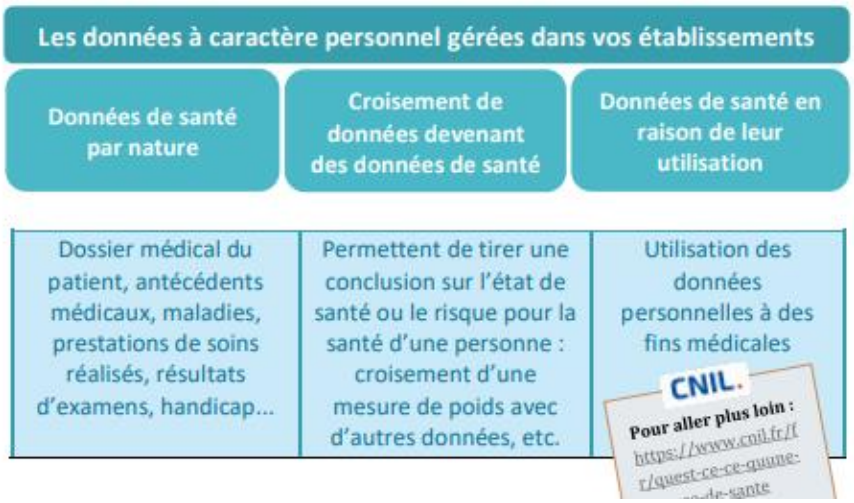
Les données de santé font partie des données à caractère personnel dites « sensibles » au sens du RGPD.

DCP sensibles Données de santé, données génétiques ou biométriques, opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle ou orientation, origine raciale ou ethnique,

DCP présentant une sensibilité particulière Numéro de sécurité sociale

DCP courantes Etat civil (date de naissance, adresse…), données de connexion (adresse IP, journaux, cookies), données de localisation

hôpital).



2- L'analyse d'impact

L'AIPD est un outil important pour la responsabilisation des organismes : elle les aide non seulement à construire des traitements de données respectueux de la vie privée, mais aussi à démontrer leur conformité au Règlement général sur la protection des données (RGPD). Elle est obligatoire pour les traitements susceptibles d'engendrer des risques élevés.

L'AIPD se décompose en trois parties :

- Une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels
- L'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quels que soient les risques ;
- L'étude, de nature plus technique, des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.

Une délibération du 11 octobre 2018 a mis en avant le fait que les établissements médico-sociaux sont obligés de se conformer au règlement européen et d'effectuer une analyse d'impact dans le cadre des traitements de données de santé. Ceux qui ne sont pas des établissements médico-sociaux doivent faire une AIPD à partir du moment où le traitement de données santé apparaît dans la liste établie par le nouveau règlement européen.

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise

Types d'opérations de traitement	Critères issus des lignes directrices du CEPD qu'ils remplissent	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.	- collecte de données sensibles - personnes dites « vulnérables »	- traitements « de santé » mis en œuvre par les établissements de santé (hôpital, CHU, cliniques, etc.) : • dossier « patients » ; • algorithmes de prise de décision médicale ; • dispositifs de vigilances sanitaires et de gestion du risque ; • dispositifs de télémédecine ; • gestion du laboratoire de biologie médicale et de la pharmacie à usage intérieur, etc. - 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).

3- L'identifiant national de santé

L'INS est un identifiant national unique pour chaque usager du système de santé. Il est constitué du numéro d'identification de l'individu au répertoire des personnes physiques (NIR ou NIA) et des traits d'identité de référence provenant de la base nationale de référence (SNGI) :

- le nom de famille,
- le(s) prénom(s) de naissance (séparés par des espaces),
- la date de naissance,
- le sexe,
- et le code géographique du lieu de naissance.

Le législateur encadre précisément l'utilisation du numéro d'inscription des personnes (NIR) au répertoire national d'identification des personnes physiques (RNIPP), en raison de la sensibilité particulière de cette donnée. Le décret « cadre NIR » définit les catégories de responsables de traitements concernés et les finalités des traitements pour lesquels l'utilisation du NIR est autorisée, notamment dans le champ de la santé.

La création d'un Identifiant National de Santé (INS) répond à une double problématique : (i) la sécurisation du référencement des données de santé afin d'éviter les doublons et les collisions de dossier tout en facilitant l'échange et le partage des données de santé et (ii) l'utilisation d'un identifiant dérivé du Numéro d'Inscription au Répertoire national d'identification des personnes physiques (NIR), ou plus communément appelé numéro de sécurité sociale.

L'utilisation du NIR comme INS des personnes pour leur prise en charge à des fins sanitaires et médico-sociales a été pour la première fois prévue par la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé, clôturant une longue réflexion commune avec la Commission Nationale de l'Informatique et des Libertés (CNIL).

Un premier décret d'application pris après avis de la CNIL le 27 mars 2017 est venu préciser les modalités d'utilisation de l'INS suivi d'un second décret en date du 8 octobre 2019 permettant

(i) de préciser le champ d'application de l'utilisation de l'INS,
(ii) la mise en conformité des dispositions règlementaires relatives à l'INS avec l'entrée en application du RGPD et
(iii) repoussant la date butoir de mise en conformité des acteurs avec les nouvelles dispositions règlementaires relatives à l'INS au 1er janvier 2021 (initialement prévue au 1er janvier 2020).

Ainsi, et conformément à l'article R. 1111-8-2 du code de la santé publique, modifié par le décret en date du 8 octobre 2019, l'INS est utilisé pour référencer « les données de santé et les données administratives de toute personne bénéficiant ou appelée à bénéficier d'un acte diagnostique, thérapeutique, de prévention, de soulagement de la douleur, de compensation du handicap ou de prévention de la perte d'autonomie, ou d'interventions nécessaires à la coordination de plusieurs de ces actes » et seulement ces données, à l'exception de la possible utilisation de l'INS à des fins de recherche dans le domaine de la santé.

Plus spécifiquement

- Sur la valeur de l'INS
  Ce second décret prévoit que le référencement des données de santé nécessite l'association de l'identifiant national de santé et d'éléments d'identité provenant du répertoire national d'identification des personnes physiques. Ainsi, l'INS a pour valeur le NIR (ou, dans le cas où la personne est en attente d'attribution de NIR, le numéro identifiant d'attente, ou NIA) auquel sont associés des traits d'identité de la personne.
  Ces dispositions ont été détaillées et développées dans le récent référentiel « Identifiant National de Santé », élaboré par l'Agence du Numérique en Santé (anciennement ASIP Santé) et approuvé par arrêté du 24 décembre 2019.
- Sur l'INS lui-même et sa nature
  Le référentiel précise que les « éléments d'identité », au sens de l'article R. 1111-8-6 du code de la santé publique sont relatifs aux nom de famille (ou naissance), prénoms, sexe, date de naissance et lieu de naissance du patient.
  L'INS n'est pas lui-même une donnée de santé mais, dès qu'il est associé à une donnée de santé, le régime juridique de la donnée de santé s'applique à lui.
- Sur le domaine d'application de l'INS
  - les données de toute personne bénéficiant ou appelée à bénéficier d'un acte diagnostique, thérapeutique, de prévention, de soulagement de la douleur, de compensation du handicap ou de prévention de la perte d'autonomie, ou d'interventions nécessaires à la coordination de plusieurs de ces actes (article R. 1111-8-2 du code de la santé publique),
  - par les personnes (i) participant à la prise en charge sanitaire ou médico-sociale et (ii) faisant partie du cercle de confiance, soit les professionnels de santé, les établissements, services, professionnels concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le code de la santé publique, les services de santé des armées, les établissement, services ou professionnels du secteur médico-social, et les professionnels concourant à une équipe de soins au sens de l'article L. 1110-12 du code de la santé publique (article R. 1111-8-2 du code de la santé publique),
  - pour des fins de prises en charge sanitaire ou médico-sociale ou afin d'assurer le suivi social ou la gestion administrative de la personne prise en charge et,
  - en l'absence de dérogation à l'obligation d'utiliser l'INS, telle que l'impossibilité de procéder au référencement (exemple : prise en charge en urgence) et l'existence d'un texte

s’opposant à l’identification (exemple : texte imposant l’anonymat).

A compter du 1er janvier 2021 les données de santé et les données administratives de toute personne bénéficiant ou appelée à bénéficier d’un acte diagnostique, thérapeutique, de prévention, de soulagement de la douleur, de compensation du handicap ou de prévention de la perte d’autonomie, ou d’interventions nécessaires à la coordination de plusieurs de ces actes devront être référencées par l’identifiant national de santé (INS).

L’objectif est double : fiabiliser le référencement des données de santé et faciliter leur échange et leur partage. Autant l’INS sera, en janvier 2021, généralisé, autant son utilisation sera restreinte à un nombre limité d’acteurs formant le “cercle de confiance”. L’INS figure parmi les référentiels socles du virage numérique

En troisième lieu, le nouveau texte renforce les règles de sécurité entourant l’accès à l’INS, en réécrivant l’article R.1111-8-6 du Code de la santé publique : il est ainsi prévu que des téléservices, mis en œuvre par la Caisse nationale de l’Assurance maladie (Cnam), permettent aux professionnels, établissements, services ou organismes d'accéder au NIR, et de « vérifier son exactitude » dans le respect d’un référentiel devant être publié d’ici la fin de l’année civile.

Par ailleurs, le recours de principe aux téléservices est désormais systématisé, sauf en cas « d'indisponibilité », ou de « motif légitime » invoqué par les professionnels.

Le décret ajoute que le recours aux téléservices n'exonère pas les professionnels, établissements, services ou organismes « de mettre en place toute procédure de surveillance, de correction et de prévention des erreurs relevant de l'organisation de la prise en charge des personnes et concourant à la maîtrise du risque d'erreur dans l'identification des personnes ».

En résumé, le nouveau texte définit les modalités de mise en œuvre de l’obligation d’utilisation de l’INS, précise les procédures de surveillance et de gestion des risques et erreurs liées à l’identification des personnes prises en charge devant être mis en œuvre par les professionnels, établissements, services et organismes, ainsi que les mesures de sécurité applicables aux opérations de référencement de données à caractère personnel concernées.

En effet, des mesures de sécurité doivent être suffisantes pour éviter que l’INS ne soit diffusé plus que nécessaire à des fins détournées, et c’est bien le risque ici ! La Cnil semble en avoir pris conscience, en demandant que soient détaillées, dans l’analyse d’impact relative à la protection des données, « les mesures de sécurité conséquentes » devant être mises en œuvre en la matière.

III- L’hébergement des données de santé

Les données personnelles de santé sont des données sensibles. Leur accès est encadré par la loi pour protéger les droits des personnes. L’hébergement de ces données doit en conséquence être réalisé dans des conditions de sécurité adaptées à leur criticité. La règlementation définit les modalités et les conditions attendues.

"Toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l’occasion d’activités de prévention, de diagnostic, de soins ou de suivi médico-social pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, doit être agréée ou certifiée à cet effet."

L.1111-8 du code de la santé publique, modifié par la loi n° 2016-41 du 26 janvier 2016

Les hébergeurs de données de santé sur support numérique (en dehors des services d’archivage électronique) doivent être certifiés.
Cette certification remplace l’agrément aujourd’hui délivré par le ministère de la Santé dans les conditions définies par le *décret n°2006-6 du 4 janvier 2006*.

Le *décret 2018-137 du 26 février 2018* définit la procédure de certification et organise la transition entre l’agrément et la certification. L’arrêté portant approbation des référentiels d'accréditation et de certification publié le 29 juin 2018 permet l’ouverture du schéma d'accréditation HDS. Les hébergeurs pourront déposer une demande de certificat HDS auprès de tout organisme de certification ayant réalisé les démarches d’accréditation auprès du COFRAC.

1- Hébergement en interne

Examinée sous le prisme du RGPD, la réglementation sur l’hébergement de donnée de santé semble ne s’appliquer qu’à l’hébergement externalisé auprès d’un sous-traitant et non à l’hébergement en interne de telles données par un responsable de traitement.

Le décret du 26 février 2018 n’apparaît pas ainsi applicable à l’hébergement « en interne » de données de santé, et ce type d’hébergement ne devrait donc pas faire l’objet d’une certification HDS, ou d’un agrément.

2- Sous-traitance

Les activités pour lesquelles un hébergeur peut être certifié sont :

1. la mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;

2. la mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;

3. la mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;

4. la mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;

5. l'administration et l'exploitation du système d'information contenant les données de santé;

6. la sauvegarde de données de santé.

Dans le cadre de la procédure d'agrément des hébergeurs de données de santé à caractère personnel précisée par le décret du 4 janvier 2006, 120 hébergeurs sont à ce jour agrées par le ministre chargé de la santé.

IV- La fonction de Directeur des Services Informatiques et le RGPD

1- Les missions et la responsabilité du DPO

Le responsable de traitement est une personne physique ou morale, autorité publique, service ou autre organisme, juridiquement responsable, qui détermine la finalité et les moyens du traitement

Le “délégué à la protection des données” en Français. Il est toutefois mieux connu sous le nom de « Data Privacy Officer » ou « Data Protection Officer »

a) missions

Les missions du DPO sont clairement définies dans le RGPD (art. 38 et 39), son rôle est de conseiller de manière indépendante le responsable du traitement et s’assurer que le RGPD est bien respecté dans l’organisation.

Dans la conduite de ses missions, il doit tenir compte en particulier des risques associés aux opérations de traitement compte tenu des données traitées et de la manière dont elles sont traitées.

Il lui incombe notamment :

- d’informer et conseiller le responsable du traitement quand aux obligations en matière de protection des données personnelles ; cela implique de mener des actions de sensibilisation et de formation
- de contrôler le respect du RGPD - au travers d’audit de mise en conformité
- dispenser des conseils sur demande - notamment en ce qui concerne la PIA
- gérer les interactions avec la CNIL (ou toute autre autorité de contrôle) et à ce titre, fait office de point de contact avec elle

En clair, le DPO a un rôle actif pour assister le responsable de traitement dans la mise en conformité de son organisation.

b) Est-il obligatoire ?

Il est obligatoire de désigner un DPO dans 3 cas :

1. si vous êtes un organisme public ou une autorité publique
2. si vous procédez à un suivi à grande échelle de personnes
3. si vous traitez des données sensibles (ex : santé) à grande échelle

Ces données sensibles sont énumérées aux articles 9 et 10 du règlement et sont, toute donnée faisant apparaître de manière directe ou indirecte :

- l'origine raciale ou ethnique des personnes ;
- les opinions politiques, les convictions religieuses ou philosophiques ;
- l'appartenance syndicale ;
- les données génétiques ;
- les données biométriques aux fins d'identifier une personne physique de manière unique ;
- les données concernant la santé ;
- les données concernant la vie sexuelle ou ;
- des données faisant apparaître l'orientation sexuelle d'une personne physique.

Les traitements à grande échelle sont des traitements "qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé,

Exemples de "traitements à grande échelle" :

- Traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités.
- Traitement des données de voyage des passagers utilisant un moyen de transport public urbain.
- Traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités ;
- Traitement des données à caractère personnel par un moteur de recherche à des fins de publicité.
- Traitement des données (contenu, trafic, localisation) par des fournisseurs de services de téléphonie ou internet.

Exemples de traitements ne constituant pas un "traitement à grande échelle" :

- Traitement, par un médecin exerçant à titre individuel, des données de ses patients.
- Traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions par un avocat exerçant à titre individuel.

c) La responsabilité du DPO

Le Délégué n'est pas responsable en cas de de non-respect du Règlement européen : le respect de la protection des données relève de la responsabilité de l'organisme qui a désigné le Délégué (responsable du fichier) ou du sous-traitant.

A savoir : en France, il existe des situations où le Délégué pourrait, comme n'importe quel autre employé ou agent, voir sa responsabilité pénale engagée :

S'il enfreint intentionnellement les dispositions pénales des règles protectrices des données personnelles.

Ou en tant que complice s'il aide le responsable du traitement ou le sous-traitant à enfreindre ces dispositions pénales.

2- Le DSI peut-il être DPO

Trop souvent, on estime que la conformité au RGPD concerne le service informatique, car il possède vos données personnelles et votre technologie. Mais la conformité doit être un engagement à l'échelle de l'association ou de l'entreprise.

Conditions

- Interne ou externe, le Délégué doit posséder des connaissances spécialisées de la législation et des pratiques en matière de protection des données. Son niveau d'expertise doit être adapté à l'activité de l'organisme pour lequel il est délégué et à la sensibilité des fichiers qui y sont mis en oeuvre.
- Le Délégué doit avoir une connaissance du secteur d'activité et de l'organisme pour lequel il est désigné.
- Il ne doit pas avoir de conflit d'intérêts avec ses autres missions.
- Enfin, le Délégué doit pouvoir exercer ses missions en toute indépendance au sein de l'organisme qui l'a désigné (capacité de faire valoir ses observations au plus haut niveau de l'organisme, animer un réseau de relais au sein des filiales d'un groupe ou encore une équipe d'experts en interne (expert informatique, juriste, expert en communication, traducteur, etc.).

La CNIL répond clairement

Un Délégué à la protection des données doit réunir certaines qualités parmi lesquelles l'absence de conflit d'intérêts avec les autres missions qu'il exerce au sein de l'organisme lorsque cette fonction est exercée à temps partiel.

Le Délégué ne peut occuper un poste qui le conduirait à déterminer les finalités et les moyens d'un fichier : en d'autres termes, il ne peut pas être "juge et partie".

Exemples de fonctions qui pourraient donner lieu à un conflit d'intérêts (appréciation au cas par cas) :

- Secrétaire général, directeur général des services, directeur général, directeur opérationnel, directeur financier.
- Médecin-chef.
- Responsable du département marketing, responsable des ressources humaines ou responsable du service informatique.

3- L'apport du DSI

Aucun individu ou service seul ne peut rendre une entreprise conforme. Cependant, dans les discussions de planification relatives à la conformité au RGPD, le service informatique ajoute une valeur importante dans des domaines évidents.

a) Apprendre à maîtriser les données

La valeur potentielle des données pour les entreprises augmente sans cesse. Cependant, de nombreux services, unités opérationnelles, voire membres du conseil ne comprennent peut-être pas à combien de données ils ont accès, où elles se trouvent, comment elles sont créées, comment elles peuvent être utilisées et comment elles sont protégées. Le service informatique peut jouer un rôle évident pour aider les entreprises à comprendre l'importance des données, et par extension du RGPD, et à déterminer la meilleure manière de les utiliser et de les protéger.

b) Assurer la sécurité des données

Le RGPD considère la protection des données personnelles comme un droit fondamental humain. Les entreprises doivent veiller à comprendre à quelle données personnelles elles ont accès et mettre en place les mesures de protection appropriées. Le service informatique a un rôle à jouer : aux côtés de l'entreprise, il doit évaluer les risques de sécurité et veiller à ce que les mesures de protection appropriées, comme le chiffrement, les contrôles d'accès, la prévention des attaques et la détection, soient mises en place.

Aider l'entreprise à être réactive

Le RGPD requiert non seulement que les entreprises protègent les données personnelles, mais aussi qu'elles répondent aux demandes des personnes qui, entre autres, souhaitent modifier ou supprimer les données détenues les concernant. Leurs données personnelles doivent donc être recueillies, rassemblées et structurées de manière à permettre un contrôle efficace et fiable de toutes ces informations. Il faut ainsi diviser les silos internes et veiller à ce qu'une entreprise possède une vision claire de ses activités de traitement en matière de données personnelles.

c) Identifier les meilleurs outils pour la tâche

La conformité au RGPD concerne autant les processus, la culture et la planification que la technologie. Cependant, certains des produits proposés peuvent aider les entreprises dans des éléments clés de la conformité au RGPD, comme la gestion des données, la sécurité et la mise en œuvre automatisée de mesures de sécurité. Grâce aux avancées dans l'automatisation et l'intelligence artificielle, de nombreux outils offrent un niveau de proactivité et d'évolutivité qui n'amoindrit pas les responsabilités envers les personnes de l'entreprise, mais peut réduire la charge de travail et mettre en place une approche capable d'évoluer selon les nouvelles exigences en matière de conformité.

d) Percevoir le potentiel

Il faut cesser de percevoir le RGPD comme un coût et commencer à y voir l'occasion d'améliorer leurs activités.

Je suis à votre disposition pour toute question et pour vous accompagner dans la poursuite de la conformité RGPD.

Sandrine MINNE

Avocat Spécialisée