PROTECTION DES DONNÉES DANS LE MÉDICO-SOCIAL

La Cnil publie un vade-mecum du RGPD

© Julien Eichinger / stock.adobe.com

Un nouveau référentiel guide les établissements et services médico-sociaux pour personnes âgées, en situation de handicap ou en difficulté, dans leurs démarches de mise en conformité et les aide à réaliser l'analyse d'impact relative à la protection des données, obligatoire au 24 mai prochain.

Bientôt le troisième anniversaire du règlement général sur la protection des données (RGPD), le 25 mai… Un référentiel de la Commission nationale de l'informatique et des libertés (Cnil) publié au Journal officiel du 23 mars va jouer un rôle de vade-mecum pour les établissements et services médico-sociaux. « *Relatif aux traitements de données à caractère personnel dans le cadre de l'accueil, l'hébergement et l'accompagnement social et médico-social des personnes âgées, des personnes en situation de handicap et de celles en difficulté* », il concerne par exemple les Ehpad, maisons départementales pour les personnes handicapées, conseils départementaux, centres communaux d'action sociale, services d'aide et d'accompagnement à domicile et de soins infirmiers à domicile.

Deux objectifs principaux

Ce référentiel répond à deux objectifs principaux : guider les professionnels dans leurs démarches de mise en conformité avec les principes informatique et libertés et les aider à réaliser une analyse d'impact relative à la protection des données (AIPD). L'AIPD est un outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée, il est obligatoire lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Ce qui est le cas pour les Ehpad : attention, la date limite est le 24 mai prochain (voir interview d'Éric Barbry).
Non contraignant lui-même, le référentiel a vocation à donner davantage de sécurité juridique aux organismes et à actualiser les anciens cadres de références adoptés avant l'entrée en vigueur du RGPD le 25 mai 2018, tels les autorisations uniques (AU) et les actes réglementaires uniques (RU).
Pour les Ehpad, il reprend la plupart du contenu de l'AU-47 (accompagnement et suivi social et médico-social des personnes handicapées et des personnes âgées) et du RU-63 (gestion de l'allocation personnalisée d'autonomie et de l'aide sociale à l'hébergement), mais à la suite de la consultation publique menée entre le 12 octobre et le 1er décembre 2020, de nouvelles précisions ont été ajoutées notamment sur : les bases légales qui peuvent être retenues dans le secteur social et médico-social, les données susceptibles d'être collectées, les durées de conservation, les destinataires, l'information et les droits des personnes concernées.

Les six finalités de traitement

Certaines finalités ont également été regroupées. Le référentiel en liste six, de façon non exhaustive :
- fournir les prestations définies dans le cadre d'un contrat conclu entre l'organisme et la personne concernée ou son représentant légal et, le cas échéant, assurer la gestion du dossier administratif de la personne concernée (gestion des rendez-vous médicaux et/ou sociaux, des visites familiales, etc.) ;
- instruire, gérer et, le cas échéant, ouvrir les droits et/ou verser les prestations sociales légales et facultatives ;
- offrir un accompagnement social et médico-social adapté aux difficultés rencontrées ayant notamment pour objet d'élaborer un projet personnalisé d'accompagnement au regard des habitudes de vie, des demandes particulières, des besoins particuliers, de l'autonomie physique et psychique de la personne et d'en assurer le suivi, d'assurer le suivi des personnes dans l'accès aux droits et, le cas échéant, d'orienter les personnes vers les structures compétentes susceptibles de les prendre en charge ;
- échanger et partager les informations strictement nécessaires, dans le respect des dispositions légales, afin de garantir la coordination et la continuité de l'accompagnement et du suivi des

personnes entre les intervenants sociaux, médicaux et paramédicaux ;
- assurer la gestion administrative, financière et comptable de l'établissement, du service ou de l'organisme ;
- assurer la remontée des informations préalablement anonymisées aux autorités compétentes concernant des dysfonctionnements graves ou événements ayant pour effet de menacer ou de compromettre la santé, la sécurité ou le bien-être des personnes prises en charge, établir des statistiques, des études internes et des enquêtes de satisfaction aux fins d'évaluation de la qualité des activités, des prestations et des besoins à couvrir.

Bases légales et durées de conservation

Le référentiel précise que chaque finalité doit reposer sur l'une des bases légales prévues par l'article 6 du RGPD. Pour aider les responsables de traitement, il propose un tableau des bases légales les plus courantes. La Cnil attire toutefois l'attention des ESMS sur la nécessité de faire preuve de prudence lorsqu'ils utilisent le consentement comme base légale de leurs traitements de données. Les personnes âgées, en situation de handicap ou de difficulté, « *peuvent en effet souffrir d'altération du discernement* ». De manière générale, le responsable de traitement doit veiller au respect des conditions de recueil du consentement et plus particulièrement « *au caractère libre, spécifique, éclairé et univoque du consentement* ».
Par ailleurs, en vertu du principe de minimisation des données, le responsable de traitement doit veiller à ce que seules les données nécessaires à la poursuite des finalités du traitement soient effectivement collectées et traitées.

Un tableau fournit des illustrations des données que la Cnil considère comme étant en principe adaptées selon les finalités du traitement.
En amont de la réalisation du traitement, le responsable du traitement doit déterminer la durée de conservation des données, deux ans en principe.
Le référentiel propose un tableau comportant des exemples de durée adéquate. À titre d'illustration, pour l'accompagnement médico-social de la personne concernée, le dossier médical peut être conservé deux ans en base active, à compter du dernier contact avec la personne concernée et vingt ans en archivage intermédiaire, à compter de la date du dernier séjour de son titulaire au sein de l'établissement de sa prise en charge.

Catherine Maisonneuve

Trois questions à Éric Barbry, avocat

Les Ehpad ont une obligation particulière : l'analyse d'impact relative à la protection des données (AIPD) portant sur les dossiers des résidents. Le point avec Éric Barbry, avocat associé IP-IT & Data Protection du cabinet Racine.

En quoi consiste l'analyse d'impact ?
A analyser de manière approfondie, article par article, le respect du RGPD pour tel ou tel traitement de données. Attention, l'AIPD n'est pas une analyse de risque ou un audit de sécurité mais une appréciation 360° de la conformité du traitement.
Elle est donc essentiellement juridique (fondement, minimisation, durée de conservation, droit des personnes, information des personnes, etc.) et comprend une partie « organisationnelle » et une partie « technique ».
Le tout doit aboutir à une maîtrise des risques : divulgation non autorisée, altération des données, modification des données, suppression, etc.

Pourquoi les Ehpad ?
Les analyses d'impacts sont essentiellement requises lorsque le traitement fait porter un risque particulier pour les droits et les libertés des personnes.
Il existe deux cas principaux dans lesquels l'analyse d'impact est obligatoire : lorsque le RGPD l'impose ou lorsqu'une autorité de contrôle (chez nous la Cnil) l'impose.
Or, pour le cas particulier des Ehpad, la liste établie par la Cnil précise qu'une analyse d'impact est obligatoire pour les « *traitements portant sur les dossiers des résidents* ».
Cette obligation vient d'être rappelée au point 11 du nouveau référentiel publié le 23 mars dernier.

Mais il faut se dire que dans 99 % des cas, identifier les trous dans la raquette revient à corriger le tir immédiatement pour réduire les risques à un niveau acceptable, je l'ai vérifié avec les entreprises dont je suis le DPO [Data protection officer, ou DPD, délégué à la protection des données].

Peut-être certains Ehpad espèrent-ils passer entre les gouttes…
Attention ! Lors de l'adoption du RGPD, la Cnil avait accordé un délai de grâce de trois ans pour se mettre en conformité. Il expire le 24 mai 2021 à minuit. Certes, pour l'heure, la Cnil n'a pas procédé à des contrôles mais à n'en pas douter, elle le fera à compter du 25 mai. Les Ehpad ne doivent pas mettre la poussière sous le tapis ! Les sanctions prévues sont lourdes, 2 % du chiffre d'affaires, le risque encouru est donc démesuré par rapport à l'investissement que représente l'AIPD. Et il est encore temps pour les retardataires de s'y atteler, ils n'auront pas forcément la malchance d'être parmi les premiers contrôlés…