(Lecture seule) ASH3051_P022_025_MANAGE_42-MAG-Decrypt 07/03/18 16:09 Page22

Etablissements médico-sociaux

Protection des données personnelles
Alerte générale

Le 25 mai 2018, entrera en vigueur le nouveau règlement européen – transcrit en droit français – sur la protection des données personnelles. Pour toutes les entreprises et donc pour les établissements et services sociaux et médico-sociaux, c'est à la fois un défi, parce que les mesures techniques sont complexes, et un changement de paradigme, parce que, d'une logique déclarative, on passe à une logique de responsabilité. Le non-respect de ces obligations est passible de lourdes sanctions financières et pénales. Explications.

Un casse-tête ? Une usine à gaz ? Une nouvelle couche au millefeuille réglementaire ? A l'instar de l'ensemble des entreprises publiques ou privées, les établissements et services sociaux et médico-sociaux (ESSMS) devront être en conformité avec le règlement général sur la protection des données (RGPD) – et ses 99 articles – au 25 mai 2018. C'est donc la dernière ligne droite pour engager ce chantier imposé par l'Union européenne. Un chantier que les ESSMS, déjà soumis, au fil des années, à une inflation normative, retardent, rechignent ou redoutent à lancer.

M. NUNES

Pascal Lefèbvre, consultant

« Un grand nombre d'entreprises françaises ne seront pas prêtes à cette échéance. Mais la présidente de la Commission nationale de l'informatique et des libertés [CNIL] *a déclaré qu'il y aurait de la souplesse en matière de contrôles en 2018 »*, rassure David Luponis, spécialisé en cybersécurité et en sécurité des systèmes d'information, associé au cabinet d'audit et de conseil Mazars. *« La priorité est de démontrer à la CNIL que le sujet RGPD est en cours de traitement »*, ajoute-t-il.

Chaque jour, les ESSMS collectent, traitent, partagent et stockent de nombreuses données à caractère personnel sous formats papier et numérique (données de ressources humaines, données sur les résidents-usagers, les bénévoles, les partenaires) et des données sensibles telles que les données de santé. Avec le RGPD, protéger les données personnelles des résidents, des mineurs, des salariés devient un enjeu majeur. *« Le RGPD n'arrive pas sur un terrain vierge, sur une lune stérile où tout serait à construire. Il ne fait que reprendre la plupart des principes et préceptes existants dans la loi "Informatique et libertés" tout en renforçant les droits des personnes sur le volet de l'information et du consentement »*, souligne Pascal Lefebvre, consultant dans les secteurs du médico-social et de l'action sociale du cabinet Lefebvre-Conseils.

« Les établissements médico-sociaux sont déjà sensibilisés aux problématiques de confidentialité des données de leurs résidents et de cybersécurité. Mais avec l'entrée en application de ce règlement européen, le niveau d'obligations auquel ils seront soumis sera sensiblement renforcé. Ils devront mettre en place des mesures de protection des données appropriées et démontrer à tout moment qu'ils sont en conformité avec la législation, tout comme leurs sous-traitants », explique David Luponis.

En dépit de leurs craintes et de leurs réticences, les ESSMS ont tout à gagner à prendre très au sérieux la mise en œuvre du RGPD et à l'inscrire au rang de leurs

Avec le RGPD, protéger les données personnelles des résidents, des mineurs, des salariés devient un enjeu majeur

(Lecture seule) ASH3051_P022_025_MANAGE_42-MAG-Decrypt 07/03/18 16:09 Page23

ZINKEVYCH/ADOBE STOCK

priorités de 2018. En effet, si la loi « Informatique et libertés » se basait sur du déclaratif initial et des contrôles ponctuels de la CNIL, la philosophie du nouveau règlement européen est résolument tournée vers la responsabilisation des entreprises (principe d'« *accountability* »). En clair, il appartiendra aux gestionnaires d'ESSMS de prendre toutes les mesures organisationnelles, techniques et juridiques requises pour garantir la conformité du traitement des données personnelles et de pouvoir le démontrer… à tout moment.

LE RÈGLEMENT EST UNE CHANCE

« Pour les établissements qui traitent des données sensibles, la notion de confidentialité sera davantage renforcée. Pour se mettre en conformité avec le RGPD, ils devront franchir non pas une mais deux marches. Enfin, l'exigence sera accrue et des attentes plus élevées pour les structures qui traitent des données sur les mineurs », avertit Laetitia Rault, senior manager au cabinet Mazars. *« Comme tout projet de mise en conformité, le RGPD demandera du temps. Il faudra compter entre 18 et 24 mois pour créer ou réorganiser des procédures internes garantissant la protection des données, mettre en place une politique de sensibilisation et de formation du personnel aux règles de sécurité et de confidentialité. Ce temps sera nécessaire pour inscrire ces nouvelles pratiques professionnelles dans les mœurs. Ce d'autant plus que, dans le secteur social et médico-social, il y a un fort taux de* turn-over *du personnel »*, ajoute-t-elle.

La philosophie du nouveau règlement européen est résolument tournée vers la responsabilisation des entreprises

Pour Pascal Lefebvre, le règlement général sur la protection des données doit être perçu non comme une contrainte de plus dans l'agenda des directeurs, mais comme une chance. *« Les directeurs d'établissements et services doivent avoir clairement conscience de la relation d'interdépendance qui existe entre les traitements de données personnelles et la garantie de l'effectivité des droits fondamentaux des usagers. Le droit à l'information fait partie de la Charte des droits et des libertés de la personne accueillie. La protection de la vie privée est un axe de la bientraitance, c'est un droit de l'usager que de voir protéger ses données personnelles et c'est un bénéfice éthique pour les professionnels du secteur social et médico-social »*, argumente-t-il. Ces enjeux justifient l'effort de mise en conformité que les établissements du secteur social doivent fournir. **Nadia Garadji**

Un chef d'orchestre pour la protection des données

Le règlement général sur la protection des données (RGPD) donne une place primordiale à un nouvel acteur en matière de protection des données à caractère personnel : le délégué à la protection des données (ou DPD), plus couramment désigné en anglais sous les termes *« data protection officer »* (DPO). *« Le DPO est le chef d'orchestre, c'est à lui de mettre cette gestion des données à caractère personnel en musique »*, explique David Luponis, spécialisé en cybersécurité et en sécurité des systèmes d'information, associé au cabinet d'audit et de conseil Mazars. Le DPO a pour mission de s'assurer que l'établissement ou le service respecte la réglementation en matière de protection des données personnelles. Il assiste les responsables des traitements et les autres employés impliqués en les informant, en les conseillant, et aussi en « contrôlant » la mise en œuvre de leurs fichiers. Il sera le premier relais de l'organisme de contrôle, la Commission nationale de l'informatique et des libertés (CNIL) au sein de l'établissement. Quel est le profil idéal pour ce nouvel acteur ? Selon l'article 37.5 du RGPD, le délégué doit être désigné « sur la base de ses qualités professionnelles et en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir *[ses]* missions ». Le DPD/DPO ne peut pas être le directeur des systèmes d'information (DSI), car il serait à la fois juge et partie de son action, ce qui serait inacceptable déontologiquement. La direction générale qui est déjà désignée par les textes comme le responsable de traitement des données ne peut également pas remplir cette fonction.

(Lecture seule) ASH3051_P022_025_MANAGE_42-MAG-Decrypt 07/03/18 16:09 Page24

Me Betty Sfez

« Les établissements devront montrer patte blanche »

Les retardataires n'ont plus que quelques semaines pour se conformer au règlement sur la protection des données personnelles. Quelles sont les opérations essentielles à mener avant la date butoir du 25 mai ? Explications de maître Betty Sfez, avocate expert en droit du numérique et de l'innovation technologique.

PREMIERES LIGNES CONSEIL

Le règlement sur la protection des données personnelles (RGPD) entrera en vigueur le 25 mai prochain. Que risquent les établissements et services sociaux et médico-sociaux qui ne seront pas prêts à cette échéance ?

D'une manière générale, aucun secteur d'activité économique n'est encore totalement préparé à l'entrée en application du nouveau règlement européen sur la protection des données personnelles. La Commission nationale de l'informatique et des libertés (CNIL) a répété, à plusieurs reprises, que le 25 mai ne serait pas une date couperet. Cependant, les établissements et services sociaux et médico-sociaux ne doivent pas faire preuve de négligence sur ce dossier RGPD. Ils doivent démarrer dès à présent des actions. Leur priorité est d'être en capacité de démontrer qu'ils ont initié des actions et qu'ils ne sont pas au niveau zéro de la mise en conformité au 25 mai. Les plus réfractaires au RGPD devront se méfier, car ils encourent des sanctions financières très lourdes.

Par où commencer pour être en conformité ?

L'étape numéro 1 pour les responsables de structures du secteur social et médico-social est de se former pour comprendre les principes généraux du RGPD. Une des premières obligations édictées par le RGPD est la tenue d'un registre des traitements qui remplace la déclaration à la CNIL. C'est ce document qui prouvera la conformité de l'établissement ou du service en cas de contrôle de la commission. Le chantier doit donc commencer par la réalisation d'un audit *a minima* pour comprendre où la structure en est aujourd'hui en matière de protection des données personnelles. Cette analyse permet de recenser les différentes bases de données de l'établissement, d'obtenir un inventaire précis des données personnelles, ainsi qu'une cartographie des traitements. Cet état des lieux permettra de cerner les évolutions nécessaires à engager pour la mise en conformité avec le RGPD, de prioriser les mesures correctives et d'établir une feuille de route. Sur son site Internet, la CNIL donne quelques bonnes pratiques pour remplir ce document, ainsi qu'un modèle de registre de traitement.

Avec ce nouveau règlement, les ESSMS devront mettre en place une politique proactive de traçabilité et de transparence dans le traitement des données personnelles. N'est-ce pas une révolution culturelle pour le secteur social et médico-social ?

Le secteur social et médico-social est traditionnellement un secteur où la transmission orale des informations occupe une place importante. Le RGPD sera une occasion de s'engager dans la transition numérique. Le principe d'« *accountability* » *[obligation de démontrer le respect des règles relatives à la protection des données]* du règlement, issu de la culture anglo-saxonne, change la donne, avec une responsabilisation plus forte des entreprises. Les établissements devront montrer patte blanche et prouver, noir sur blanc, qu'ils ont mis en œuvre toutes les procédures internes permettant le respect des règles relatives à la protection des données.

Comment faut-il comprendre la notion de consentement dans le RGPD ?

Le consentement de la personne concernée par le traitement des données personnelles doit être libre, explicite, éclairé et non équivoque. Il doit être recueilli au début de la relation contractuelle entre l'usager et l'établissement. Le consentement peut être recueilli selon des termes simples pour s'adapter à des personnes prises en charge (mineurs, personnes sous tutelle, personnes âgées dépendantes). Par exemple avec la création d'icônes, pour leur permettre de comprendre tout de suite. Pour les mineurs, le projet de loi « informatique et libertés » 2 prévoit d'abaisser de 16 ans à 15 ans l'âge à partir duquel un mineur peut consentir seul au traitement de ses données. En dessous de cet âge, le consentement des parents sera nécessaire.

(Lecture seule) ASH3051_P022_025_MANAGE_42-MAG-Decrypt 07/03/18 16:09 Page25

Quelles opportunités le secteur social et médico-social peut-il tirer de cette réglementation?
Le RGPD est une problématique transverse de l'entreprise nécessitant la mise en place de mesures organisationnelles, techniques et juridiques. Cela va forcer les personnels et les différents services à communiquer entre eux, et améliorer le contrôle qualité. Les Français sont sensibles à la protection des données personnelles. Trois ans et demi après l'instauration du droit à l'oubli par la Commission européenne, la France est le pays dont les citoyens y ont le plus recours. Selon une étude de Google, 20,4 % des demandes de déréférencement dans l'Union européenne viennent de l'Hexagone. Par ailleurs, le nombre de plaintes auprès de la CNIL pour atteinte aux règles de protection des données personnelles a augmenté. Dans ce contexte, la mise en application du RGPD est une occasion pour les établissements de renforcer la relation de confiance avec les usagers et les familles, d'être « dans les clous » avec la réglementation et d'assurer une confidentialité totale des dossiers des résidents. **Propos recueillis par N. G.**

« Du bazar à l'ordre numérique »

« Un simple fichier Excel contenant des contacts constitue un traitement de données personnelles. Dans chaque ESSMS, parfois au sein d'une même entité juridique, chacun va développer ses propres outils de traitement de données. Combien existe-t-il de fichiers? Quelles données contiennent-ils? A quoi servent-ils? Qui y accède? A quel moment sont-ils détruits? Etablir cette cartographie sera un cauchemar pour certains délégués à la protection des données (DPD). Dans certains cas, c'est le bazar. Et quand on informatise, c'est le bazar informatisé. Le RGPD est l'occasion pour les organismes gestionnaires d'inscrire en gros dans leur politique associative la protection des données personnelles comme un enjeu stratégique. Cette nouvelle réglementation est une formidable occasion d'acculturer le secteur social et médico-social à la transition numérique », considère Myriam Vallin, consultante au cabinet de conseil Handiness, consacré à la transition numérique du secteur médico-social. •

Adef Résidences ou le bon soldat

Une structure associative a anticipé le règlement sur la protection des données (RGPD) et est prête à affronter le big bang du 25 mai.

L'association Adef Résidences, gestionnaire de 48 établissements d'hébergement pour personnes âgées dépendantes (EHPAD), maisons d'accueil spécialisées (MAS), foyers de vie et foyers d'accueil médicalisés (FAM), dispose, depuis 2003, d'une filiale consacrée à l'informatique et aux technologies de l'autonomie, baptisée Algonis. Un atout de taille pour réussir la mise en conformité au RGPD. *« Algonis a une expertise médico-sociale, une bonne compréhension des directions métiers et des établissements. Les préoccupations concernant le respect de la vie privée, la confidentialité des données personnelles et la cybersécurité font déjà partie des pratiques professionnelles dans nos établissements médico-sociaux »*, explique Olivier Rival, directeur. Et de poursuivre : *« Algonis développe elle-même des logiciels métiers pour les EHPAD, les FAM et les MAS qui respectent déjà les règles de sécurité et de protection des données personnelles. C'est le cas, par exemple, avec le logiciel de restauration Miam-I pour la préparation des repas des ESMS* [établissements sociaux ou médico-sociaux], *dans lequel les données personnelles sont anonymisées et supprimées à partir d'un certain délai, et sécurisées grâce à des accès* via *des mots de passe. Par ailleurs, les données de santé des résidents sont stockées en toute sécurité chez un hébergeur titulaire de l'agrément pour l'hébergement de données de santé à caractère personnel. »*

Olivier Rival, directeur d'Algonis DR

UN PERSONNEL FORMÉ ET SENSIBILISÉ

Les établissements d'Adef Résidences disposent de solutions logicielles qui permettent de lutter contre les cyberattaques et les logiciels informatiques malveillants, tels que les malwares et les ransomwares. Le personnel est formé et sensibilisé aux règles à respecter pour protéger l'accès aux données personnelles. La mise en œuvre du RGPD s'inscrira donc dans la continuité des actions déjà menées par l'association. *« Un délégué à la protection des données a été désigné pour organiser, légitimer et faire avancer ce chantier, et en assurer le pilotage opérationnel. Nous sommes actuellement en plein dans le travail de cartographie du traitement des données personnelles. Toutes les directions et les établissements y sont associés »*, précise Olivier Rival.

Du côté de l'association, la mise en œuvre du RGPD n'est pas vécue comme une contrainte mais comme *« une occasion de renforcer la relation de confiance avec les résidents, les familles »*. *« Le respect des règles de confidentialité est fondamental pour Adef Résidences. Cela passe par le droit à l'image de nos résidents et par la confidentialité des données personnelles, qui participent tous deux à la culture de la bientraitance »*, insiste Arnaud Gallet, directeur de la communication. *« Ce chantier est une occasion d'aller plus loin dans notre politique de protection des données personnelles. Pour les salariés des établissements médico-sociaux, c'est l'occasion d'être impliqués dans un projet transverse, collectif »*, considère Olivier Rival. **N. G.**