MYRIAM VALLIN, CONSULTANTE CHEZ HANDINESS

"Avec le RGPD, les établissements médico-sociaux doivent acquérir une culture de l'information"

Publié le 24/04/18 - HOSPIMEDIA

Le règlement européen sur la protection des données personnelles s'appliquera en France dans quelques semaines et les établissements et services médico-sociaux ont encore beaucoup à faire pour s'y conformer. Myriam Vallin, consultante chez Handiness, accompagne des structures dans cette transition et fait le point sur les enjeux et les priorités.

Hospimedia : "Le règlement européen sur la protection des données personnelles (RGPD) entre en vigueur en France le 25 mai. Les établissements et services médico-sociaux (ESMS) sont-ils prêts ?

Myriam Vallin : On peut dire qu'il y a à peu près trois cas de figure. Certains ont bien anticipé. Il faut dire que le RGPD est déjà connu depuis le 8 avril 2016. On savait de toute façon qu'il s'imposerait aux États membres en 2018 sans qu'il y ait besoin d'une ratification nationale car c'est un règlement européen. Dans les grandes lignes, on savait exactement à quoi s'attendre. Néanmoins, un tiers des ESMS a bien anticipé, un tiers commence à s'en préoccuper et un tiers espère toujours y échapper.

H. : Quelles sont les principales difficultés que rencontrent les ESMS face à l'application de ce règlement ?

M. V. : Dans la plupart des cas, les systèmes d'information (SI) sont très peu développés. Il y a une maturité insuffisante par rapport à tous ces sujets. À Handiness, lorsque l'on interroge les structures pour leur demander quelles sont les données personnelles dont elles disposent sur les personnes accueillies, les salariés et administrateurs, à quoi elles servent et qui y a accès, dans la majorité des cas elles ne savent pas. La vision du SI, avec tout ce que cela comporte, n'est pas du tout acquise. Il n'y a pas de culture globale de l'information, en conséquence, les moyens qui sont consacrés à l'informatisation sont ridicules. Et beaucoup de structures n'ont pas de responsable informatique.

H. : Face à ce constat, quelles sont les priorités pour que les ESMS se conforment au mieux au RGPD dans le temps imparti ?

M. V. : Je pense que la mise en œuvre du RGPD va justement permettre une prise de conscience pour les ESMS sur le fait qu'il faut structurer leur SI, et le structurer en imaginant que l'information va sortir des établissements pour alimenter le dossier médical partagé (DMP), le logiciel des maisons départementales des personnes handicapées (MDPH), etc. Il faut vraiment que la mayonnaise prenne. Mais ça ne se fera pas tout de suite. Cela va être long car il va y avoir une acculturation nécessaire des équipes qui est forcément longue. Techniquement, la mise en œuvre du RGPD n'est pas très compliquée mais ce qu'il faut vraiment acquérir, c'est cette culture de l'information. Par exemple, je ne souhaite pas intervenir auprès de structures qui me disent : "*Vous avez le nombre de jours qu'il faut pour mettre en œuvre le RGPD mais on ne veut pas en entendre parler.*" Je pense que c'est une énorme erreur. J'estime que mon rôle est d'accompagner la structure, de lui donner des outils, de lui permettre de s'en servir et ensuite de se débrouiller toute seule, quitte à revenir plus tard ou faire des points téléphoniques. Il y aura un accompagnement nécessaire car comme tout projet de loi qui se met en place, une jurisprudence va construire la réglementation au fur et à mesure. À partir du 25 mai, les établissements doivent prendre conscience qu'ils ont un actif de plus : les données personnelles qu'ils gèrent.

H. : Le secteur médico-social n'est pas tout à fait prêt, pourtant tout n'est pas nouveau dans le RGPD, il reprend les cinq grands principes de la loi Informatique et libertés.

M. V. : Oui et depuis il y a eu aussi la loi 2002-2 avec des procédures de consultation du dossier personnalisé, et un certain nombre de mesures à mettre en place, ce qui n'a pas forcément été fait. La plupart du temps lorsqu'une structure a un dossier informatisé de la personne accueillie, elle a procédé à une déclaration unique au niveau de la Commission nationale de l'informatique et des libertés (Cnil). Par contre, ce que les établissements n'ont pas compris, c'est que le moindre fichier informatisé devrait lui aussi faire l'objet d'une déclaration. Cette réalité date de quarante ans.

H. : Est-ce que les ESMS bénéficient d'un accompagnement pour la mise en œuvre de ce règlement ?

M. V. : À ma connaissance, il n'y a pas de financement dédié. Les ESMS ont l'impression qu'on leur demande toujours de faire plus avec moins. C'est vrai aussi, on ne peut pas le nier, il y a un manque de moyens. Ce n'est pas leur cœur de métier mais ils doivent s'en occuper, comme tout chef d'entreprise.

M. V. : Du fait des grands groupes, le secteur des personnes âgées me semble quand même moins à la pein, mais justement parce qu'il avait déjà respecté les principes de la loi Informatique et libertés. Alors que le secteur du handicap, lui, fait le grand saut à partir de rien pour arriver d'un seul coup au RGPD, sans préparation. Il y a une incompréhension des enjeux, malgré les rappels de l'actualité.

H. : Et en termes de délais ?

H. V. : Certains pensent qu'ils ont trois ans pour se mettre en conformité tout simplement parce que la Cnil a dit que ceux dont les traitements avaient déjà été déclarés disposeraient de ces trois ans. Mais cela exclut tout de même tous ceux qui ne l'ont pas fait et ils y sont quand même légion. Ce que je crains, c'est qu'il se passe la même chose qu'avec le document unique des risques professionnels. Pour sa mise en place dans les établissements, souvent des consultants sont arrivés, l'ont produit et il a ensuite souvent été rangé dans un placard. La culture du document unique, avec la place du comité d'hygiène, de sécurité et des conditions de travail (CHSCT), n'a pas été intégrée. Et ça serait vraiment dommage qu'il se passe la même chose avec le RGPD parce que cela correspond aussi à un besoin d'acculturation des équipes et ça me paraît être un bon moyen.

H. : Est-ce que la mise en place du délégué à la protection des données, ou *data protection officer* (DPO), va être une grande difficulté pour les ESMS ?

M. V. : Cela va être une difficulté pour tout le monde, pas seulement pour les établissements médico-sociaux. Je crois qu'en 2018 on va rechercher 80 000 DPO, et on ne les a pas. Ça va être un peu plus compliqué dans les petites structures parce qu'il y a quand même un conflit d'intérêts. Le responsable informatique, quand il existe, ne peut pas être DPO puisqu'il participe à la sécurité des traitements et qu'il ne peut pas être juge et partie. C'est pareil pour le directeur des ressources humaines car il traite aussi beaucoup de données personnelles pour les salariés. Selon la configuration des structures, il va falloir essayer de trouver un profil qui convienne. En plus, dans la plupart des établissements, il n'y a pas de correspondant informatique et libertés. Ceux qui se sont bien emparés du sujet sont justement ceux qui en ont un.

H. : Est-ce qu'il sera possible de mutualiser cette fonction de DPO ?

M. V. : Oui, par contre cela va être compliqué pour un DPO d'être à la fois sur de la grande distribution et du handicap. Lorsque l'on met en place ce genre de réglementation et de culture il y a trois éléments qui comptent : le côté juridique, le côté technique et le côté métier. Les secteurs médico-social et de la santé sont particuliers, et comportent en plus beaucoup de données sensibles. Externaliser oui, pourquoi pas. Sachant qu'il faut que tout le monde soit bien d'accord sur le contrat au départ, parce que le DPO devra être au courant de ce qui se passe dans la structure. Cela veut dire qu'il faudra qu'il lise tous les comptes rendus de comité de direction, pour savoir si de nouveaux traitements vont être mis en place. Il va falloir bien caler cet aspect-là des choses. La mise en œuvre du RGPD, c'est la conquête de l'Ouest. On va forcément se retrouver à défricher, à trouver des solutions. Lorsque l'on part de rien, on doit appliquer la règle des 80/20. On va prendre les 20% de cas qui génèrent les 80% de risques et commencer par traiter ceux-là. Je pense qu'en plus la Cnil sera à l'écoute. Mais les établissements vont devoir s'y mettre, ils ne peuvent pas espérer être oubliés."

Propos recueillis par Cécile Rabeux
Ecrire à l'auteur - Twitter
