ANALYSE DU DÉCRET HDS

Mai 2018

Association Française des Hébergeurs Agréés de Données de Santé à caractère personnel

ANALYSE DU DÉCRET PORTANT SUR L'HÉBERGEMENT DE DONNÉES DE SANTÉ

A l'occasion d'une procédure qui devait être au départ purement technique, le remplacement du processus d'agrément des hébergeurs de données de santé par un processus de certification, le Ministère de la Santé a procédé à une redéfinition en profondeur des obligations des hébergeurs.

Dans la définition en vigueur depuis le décret de 2005, l'hébergeur de données de santé cumulait :

- Un rôle technique de fournisseur de ressources, correspondant à l'acceptation générale du terme d'hébergeur.
- Des obligations spécifiques portant sur les droits des patients et sur les mesures de sécurité mises en œuvre pour préserver leurs données, notamment en termes d'authentification des utilisateurs et de traçabilité des accès.

Pour faire disparaitre ces obligations spécifiques, il a fallu dans le décret remanier profondément les textes existants, avec la réécriture complète de toute la sous-section du Code de la Santé Publique portant sur l'hébergement de données de santé.

Les impacts de cette réécriture peuvent se classer en cinq volets :

- La redéfinition du périmètre de l'hébergement de données de santé
- Les mesures techniques de remplacement de l'agrément par la certification
- Le report du dossier d'agrément au contrat d'un certain nombre d'exigences
- La suppression des exigences de sécurité propres au fonctionnement de l'application
- La rupture des engagements de l'hébergeur envers la personne concernée

La redéfinition du périmètre de l'hébergement de données de santé

Le texte d'origine ne précisait pas en quoi consistait la prestation d'hébergement, se contentant de renvoyer à la mention qui en était faite dans l'article législatif L1111.8.

Dans la nouvelle rédaction (R1111-9), l'hébergement est défini comme l'exercice d'une ou plusieurs activités parmi : colocation, mise à disposition d'infrastructure matérielle, mise à disposition d'infrastructure virtuelle, mise à disposition d'une plateforme d'hébergement d'applications, administration et exploitation du système d'information, sauvegardes.

Cette énumération restrictive est risquée dans un contexte technique en perpétuelle mutation ; on peut par exemple s'interroger sur la catégorie dans laquelle tomberait la gestion de conteneurs applicatifs. Elle est sans doute motivée par la nécessité d'agglomérer dans un cadre unique des prestations de nature différente : immobilières et financières (colocation, mise à disposition de serveurs physiques) ou informatiques.

L'inclusion de l'administration et de l'exploitation du système d'information est déconcertante, puisqu'il n'intervient plus ici la moindre notion d'hébergement. En l'état

actuel, le prestataire de proximité assurant le support d'un cabinet médical ou un éditeur administrant à distance un serveur déployé dans un établissement seront ainsi soumis à la certification hébergeur.

On notera enfin la disparition de l'obligation qui figurait au R1111-9 4° de dissocier les moyens de traitement de l'hébergement de données de santé de ceux d'autres activités. Cela va évidemment dans le sens de la banalisation de l'hébergement de données de santé qui inspire ce texte.

Les mesures techniques de remplacement de l'agrément par la certification

Ces reformulations ne présentent pas de difficulté particulière. En tant que mécanisme, la certification est indiscutablement préférable à l'agrément, car plus efficace et plus complète. L'examen de la politique de sécurité, les contrôles, les processus de renouvellement, de suspension et de retrait sont transférés aux organismes certificateurs.

Le transfert du dossier d'agrément au contrat d'un certain nombre d'exigences

La disparition du dossier d'agrément implique que nombre de détails sur la prestation d'hébergement sont reportés dans les contrats passés entre l'hébergeur et ses clients. Ceci donnera plus de souplesse à l'hébergeur pour faire évoluer sa prestation au fil du temps, ce qui est un progrès.

On transpose donc au contrat la définition de la prestation, l'identification des sous-traitants, les indicateurs de qualité et de performance, les obligations en cas d'évolution, les garanties en cas de défaillance de l'hébergeur, la procédure de réversibilité.

Quelques éléments de dossier disparaissent au passage, mais cela ne pose guère de problème : identification des personnes en charge de l'activité, comptes prévisionnels.

La suppression des exigences de sécurité propres à l'application

Avec la suppression des 2° et 3° de l'article R1111-14, l'hébergeur ne doit plus s'engager dans sa politique de sécurité sur les procédés techniques d'identification et d'authentification, la gestion des habilitations et de la traçabilité des accès ou la pérennité des données au fil des évolutions techniques. Ces considérations reviennent au seul responsable de traitement, soit en l'occurrence le professionnel ou l'établissement de santé utilisateurs du service hébergé.

La rupture des engagements de l'hébergeur envers la personne concernée

Les obligations de l'hébergeur envers la personne concernée qui figuraient au 1° du R1111-14 disparaissent : condition de recueil des consentements, droits de consultation et de rectification de ses données, signalement des incidents à la personne concernée, fourniture à la personne concernée de l'historique de l'accès à ces données.

Hormis le dernier, ce sont des droits que la personne peut continuer d'exercer auprès du responsable du traitement. Ce n'est que le contrôle a priori de l'hébergeur qui disparait.

L'historique d'accès aux données pourrait peut-être réapparaitre ultérieurement via le référentiel opposable d'imputabilité prévu par les textes, mais celui-ci n'est encore pas même esquissé.

Conclusion

Ce nouveau régime vise à la banalisation de l'hébergement de données de santé. Il sert les intérêts des grands hébergeurs généralistes, qui souhaitent pouvoir proposer à grande échelle un service uniforme ne requérant pas de mobiliser une expertise pointue pour accompagner les responsables de traitement dans la mise en conformité de leurs applications.

Les perdants sont multiples :

- Les patients, qui perdent un contre-pouvoir effectif et compétent dans la mise en œuvre des traitements les concernant.
- Les établissements et professionnels de santé, qui sont quasiment toujours les responsables de traitement et vont devoir assumer les obligations et risques du nouveau règlement européen sur la protection des données personnelles sans pouvoir compter sur l'assistance experte des hébergeurs.
- Les startups et petits éditeurs, d'une part car les acteurs précédents joueront la sécurité perçue en s'adressant aux industriels les plus en vue, d'autre part parce qu'ils seront désormais tenus d'obtenir une certification pour leur activité d'administration de leurs solutions.
- Les hébergeurs spécialistes de la donnée de santé, qui ont organisé leur offre et leur structure en fonction des exigences plus ou moins pertinentes de l'agrément, pour se voir finalement devoir les défendre seuls après le lâchage par l'Etat.

Et la grande victime est la sécurité des données personnelles de santé. Espérer l'améliorer et en réduire le coût en déléguant à des milliers de responsables de traitements peu ou pas formés et sous une contrainte budgétaire écrasante les responsabilités qu'exerçaient une cinquantaine d'industriels ou de grandes directions du système d'information compétents et organisés en conséquence est un calcul pour le moins hasardeux.