CERTIFICATION HDS ET RGPD

Mai 2018

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

CERTIFICATION HÉBERGEMENT DE DONNÉES DE SANTÉ ET RGPD : UNE ANALYSE COMPARATIVE

Le remplacement de l'agrément des hébergeurs par une certification intervient quasiment simultanément avec la mise en application du Règlement Général sur la Production des Données (RGPD). Il existe entre les deux un certain nombre de similarités, de points d'accroche, mais également de divergences qui méritent d'être clarifiés.

Le fait de le soumettre à une certification fait partie des prérogatives nationales permises (Article 9).

Le périmètre obligeant à détenir une certification HDS est limité aux données recueillies à l'occasion d'activités de prévention, de diagnostic, de soins, ou de suivi social et médico-social. Il est donc bien moins étendu que celui des données de santé du RGPD, qui au considérant 35 précise que la nature de données de santé est indépendante de leur source.

L'hébergeur de données de santé (HDS) est un sous-traitant au sens du RGPD.

Sous le régime instauré par le RGPD, le sous-traitant est soumis à des obligations et des sanctions administratives directes, alors qu'auparavant celles-ci ne s'appliquaient qu'au responsable de traitement, celui-ci devant ensuite s'appuyer sur la contractualisation avec ses sous-traitants pour leur en répercuter une partie. Ce n'est toutefois pas une grande nouveauté pour les hébergeurs déjà agréés, dont l'activité dépendait de leur aptitude à respecter les critères de l'agrément.

Obligations structurelles

Par définition, l'activité d'un HDS consiste à traiter à grande échelle des données sensibles. A ce titre, il doit impérativement désigner un Délégué à la Protection des Données (Article 37) et effectuer une analyse d'impact relative à la protection des données (Article 35).

Pour donner suite à cette analyse d'impact, il est tenu de mettre en œuvre et de tester régulièrement les mesures de sécurité correspondant à son service (Article 32). Cela peut se limiter à des dispositions de sécurité physique et environnementale pour un site de colocation, ou intégrer tous les mécanismes et procédures d'utilisation et d'exploitation des traitements hébergés si son service va jusque-là.

Ces obligations sont cohérentes avec celles de l'agrément hébergeur, puis de la certification HDS, qui toutes deux reposent avant tout sur l'analyse des risques effectuée par l'hébergeur.

Ses personnels sont soumis à une obligation de confidentialité. Ceci est de toute façon déjà une obligation légale au titre de l'article L1111-8 du Code de la Santé Publique, qui astreint les personnels des HDS au secret professionnel.

Outre le registre de ses propres traitements, il doit tenir un registre des traitements hébergés. La dérogation pour les entreprises de moins de 250 personnes ne s'applique pas ici. Le détail de ce registre sera traité dans le chapitre suivant.

Obligations liées à chaque traitement hébergé

Avant l'hébergement

La relation entre l'HDS et le responsable de traitement doit faire l'objet d'un contrat écrit, reprenant la caractérisation du traitement sous-traité, le type de données à caractère

personnel et les catégories de personnes concernées, les obligations et les droits du responsable de traitement.

L'HDS doit aider le responsable de traitement à respecter ses propres obligations préalables en matière de mesures de sécurité, analyse d'impact, voire consultation préalable de la CNIL si le traitement s'avérait particulièrement risqué. Cette aide peut se limiter à la fourniture d'un dossier standardisé correspondant à la prestation sous-traitée, ou dans l'esprit de l'agrément originel aller en profondeur dans l'analyse des particularités du traitement. C'est l'objet du code de l'AFHADS que de maintenir ce niveau de service.

Le registre tenu par l'HDS doit comporter pour chaque traitement hébergé les noms et coordonnées du responsable de traitement. Il y a là une difficulté particulière, car bien souvent le client de l'HDS est lui-même un sous-traitant, offreur d'un service auprès d'établissements ou de professionnels de santé qui sont les responsables de traitement. Un mécanisme approprié permettant de propager les coordonnées des responsables de traitements vers l'HDS devra être imaginé et mis en œuvre.

Les autres items du registre sont :

- Les catégories de traitement effectuées par l'HDS
- Les éventuels transferts vers des pays tiers ou organisations internationales
- Dans la mesure du possible, les mesures de sécurité propres au traitement. La restriction à la mesure du possible dédouane les hébergeurs de cette obligation, mais elle est renforcée par le code de l'AFHADS.

Pendant l'hébergement

L'hébergeur ne traite les données que sur instruction documentée du responsable de traitement. Typiquement, la mise à disposition de sauvegardes ou d'extraction devra forcément faire l'objet d'une demande formalisée.

Il a un devoir d'aide au responsable de traitement sur ses obligations de sécurité, en tenant à jour son analyse d'impact et ses mesures de sécurité. Le code de l'AFHADS requiert également un réexamen des mesures propres à chaque traitement tous les trois ans.

L'hébergeur doit contribuer à l'obligation de notification des violations tant à la CNIL qu'aux personnes concernées. A ce titre, il doit lui-même s'engager à notifier son client des violations qu'il constaterait.

Egalement, il doit alerter son client si les instructions données par celui-ci le mettaient en défaut au regard du RGPD. Ce pourrait par exemple être le cas d'un client éditeur qui souhaiterait obtenir une extraction des données pour l'anonymiser avant une analyse statistique, alors que ce traitement n'a pas été déclaré initialement.

Enfin, il doit assister son client pour l'exercice des droits de la personne concernée : information, accès, rectification, effacement ou limitation, portabilité des données. C'est notamment à cet effet que le code de l'AFHADS prévoit le maintien du médecin de l'hébergeur, qui n'est plus requis dans le cadre de la certification.

Il doit collaborer à la réalisation d'audits et d'inspections par le responsable de traitement.

En fin d'hébergement

L'HDS doit en fin de contrat d'hébergement restituer les données au responsable de traitement (ou en cas de cascade de sous-traitance, les restituer à son client, qui lui-même assumera leur reprise ou leur restitution), et détruire l'ensemble des sauvegardes ou archives qu'il détiendrait.

Obligations liées à la sous-traitance

L'HDS ne doit pas recourir lui-même à une sous-traitance relative au traitement confié sans autorisation écrite du responsable de traitement. Il doit par ailleurs propager à ses sous-traitants les obligations issues de sa relation avec son client.

Par sous-traitance, il faut entendre la réalisation d'une partie du traitement confié. La société d'entretien des locaux doit certes présenter des garanties envers l'hébergeur ; elle n'est pas pour autant un sous-traitant du traitement hébergé dont le choix devrait être validé par chacun de ses clients.

Comparaison

Le référentiel de certification des HDS est composé de l'ISO 27001, d'exigences complémentaires piochées dans le référentiel ISO 20000 (ITIL) et les codes de bonnes pratiques ISO 27017 et 27018, et de quelques spécialisations ou exigences spécifiques figurant directement dans le référentiel d'exigences HDS.

La certification HDS n'est pas une certification de conformité au RGPD telle que prévue par l'article 42. D'une part, elle est plus large et comporte tout un volet d'exigences organisationnelles et opérationnelles qui sont en dehors du périmètre du RGPD. D'autre part, la comparaison récapitulée dans le tableau ci-après montre de nombreuses convergences. On espère que, de la même manière qu'une certification 27001 préexistante facilite concrètement l'obtention d'une certification HDS, les futures certifications RGPD sauront reconnaitre les acquis de la certification HDS.

RGPD	Certification HDS
Délégué à la protection des données	Code AFHADS pour ses membres
Analyse d'impact sur la vie privée	ISO 27001 – 6.1.2 (Analyse de risque)
Mise en œuvre et contrôle mesures de sécurité	ISO 27001 – 8.1
Engagement de confidentialité des personnels	Code de la Santé Publique – L1111-8 ISO 27001 – A.7.1.2 ISO 27018 – A10.1
Registre des traitements hébergés	Code AFHADS pour ses membres
Contractualisation	ISO 27017 – 6.1
Traitement selon instructions documentées	ISO 27018 – A2.1
Aide aux obligations préalables	Code AFHADS pour ses membres
Aide aux obligations en vie courante	Code AFHADS pour ses membres
Notification des violations	ISO 27018 – A9.1
Alerte en cas d'instruction invalide	Code AFHADS pour ses membres
Exercice des droits de la personne concernée	ISO 27018 – A1 Médecin de l'hébergeur (code AFHADS)
Collaboration aux audits	Référentiel d'exigences HDS – 4.6.2
Restitution des données	ISO 27018 – A9.3
Déclaration des sous-traitants	ISO 27018 – A7.1
Obligations des sous-traitants	ISO 27001 – A15.1