EUROPEAN COMMISSION
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

Numéro de notification : 2023/0682/FR (France)

Arrêté modifiant l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel

Date de réception : 05/12/2023
Fin de la période de statu quo : 06/03/2024 (closed)

Message

Message 001

Communication de la Commission - TRIS/(2023) 3385

Directive (UE) 2015/1535

Notification: 2023/0682/FR

Notification d'un projet de texte d'un État membre

Notification – Notification – Notifzierung – Нотификация – Oznámení – Notifikation – Γνωστοποίηση – Notificación – Teavitamine – Ilmoitus – Obavijest – Bejelentés – Notifica – Pranešimas – Paziņojums – Notifika – Kennisgeving – Zawiadomienie – Notificação – Notificare – Oznámenie – Obvestilo – Anmälan – Fógra a thabhairt

Does not open the delays - N'ouvre pas de délai - Kein Fristbeginn - Не се предвижда период на прекъсване - Nezahajuje prodlení - Fristerne indledes ikke - Καμμία έναρξη προθεσμίας - No abre el plazo - Viivituste perioodi ei avata - Määräaika ei ala tästä - Ne otvara razdoblje kašnjenja - Nem nyitja meg a késéseket - Non fa decorrere la mora - Atidėjimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħx il-perijodi ta' dewmien - Geen termijnbegin - Nie otwiera opóźnień - Não inicia o prazo - Nu deschide perioadele de stagnare - Nezačína oneskorenia - Ne uvaja zamud - Inleder ingen frist - Ní osclaíonn sé na moilleanna

MSG: 20233385.FR

1. MSG 001 IND 2023 0682 FR FR 05-12-2023 FR NOTIF

2. France

3A. Ministères économiques et financiers
Direction générale des entreprises
SCIDE/SQUALPI - Pôle Normalisation et réglementation des produits
Bât. Sieyès -Teledoc 143
61, Bd Vincent Auriol
75703 PARIS Cedex 13

3B. Délégation au numérique en santé
Ministère de la Santé et de la Prévention
14 avenue Duquesne
75007 PARIS

4. 2023/0682/FR - S00S - Santé, équipements médicaux

5. Arrêté modifiant l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel

6. Activité d'hébergement de données de santé à caractère personnel sur support numérique

7.

8. Le présent projet d'arrêté modifie le référentiel d'accréditation des organismes de certification et le référentiel de certification pour l'hébergement de données de santé à caractère personnel (HDS).

Conformément aux dispositions des articles L.1111-8 et R.1111-10 du code de la santé publique, tout hébergeur de données de santé à caractère personnel (HDS), doit être titulaire d'un certificat de conformité délivré par un organisme de certification sur le fondement d'un référentiel de certification, approuvé par arrêté du ministre chargé de la santé.

Les principales modifications apportées au référentiel de certification d'hébergement de données de santé, ont pour objectif de :
- Clarifier les activités pour lesquelles les hébergeurs ont obtenu la certification, notamment en précisant la définition de l'activité d'administration et d'exploitation des systèmes de santé ;
- Améliorer la lisibilité des garanties apportées par l'hébergeur à chaque prestataire faisant appel à ses services ;
- Clarifier les obligations contractuelles de l'hébergeur ;
- Intégrer dans le référentiel de certification HDS des évolutions de la norme ISO 27001.

La version révisée du référentiel HDS propose en outre d'ajouter quatre nouvelles exigences relatives à la souveraineté des données et plus précisément :

- Restreindre le stockage des données de santé sur le territoire d'un Etat partie de l'Espace économique européen ;

Deux exigences en matière de transparence de l'hébergeur vis-à-vis de ses clients :

- L'informer de tout transfert ou accès distant aux données du client depuis un territoire situé hors de l'Espace économique européen (EEE) qui n'assure pas un niveau de protection des données adéquat au sens de l'article 45 du RGPD, et des mesures organisationnelles et techniques mises en oeuvre pour encadrer ce transfert ;

- L'informer d'une éventuelle sujétion à une réglementation extra-communautaire qui serait susceptible d'entraîner un risque d'accès aux données par un organisme situé dans un pays qui n'assure pas un niveau de protection des données adéquat au sens de l'article 45 du RGPD, et des mesures prises pour atténuer ce risque ;

Une exigence de transparence vis-à-vis de ses clients potentiels : l'hébergeur doit rendre public et tenir à jour des informations détaillées sur les éventuels transferts de données qu'il héberge vers un pays n'appartenant pas à l'EEE et sur les mesures prises pour assurer le respect du RGPD.

9. La procédure de certification obligatoire pour les hébergeurs de données de santé à caractère personnel, créée par la loi, a pour finalité de garantir aux usagers et aux professionnels de santé que ces données sensibles au sens du RGPD, confiées dans le cadre d'une prise en charge médicale, sont sécurisées.

Le présent projet d'arrêté est pris en application des articles L.1111-8 et R.1111-10 du code de la santé publique, pour approuver une version révisée : d'une part du référentiel de certification pour l'hébergement de données de santé (HDS), d'autre part du référentiel d'accréditation des organismes certificateurs, lesquels avaient été initialement approuvés par arrêté du 11 juin 2018. Le décret n° 2018-137 qui a créé les dispositions des articles R. 1111-8-8 et suivants du CSP, ainsi

que l'arrêté du 11 juin 2018, ont tous deux fait l'objet d'une notification à la Commission européenne en 2017.

Le dispositif global de certification mis en place en 2018 n'est pas modifié, seuls certains points font l'objet d'une mise à jour.
Les seules exigences ajoutées au référentiel de certification portent sur la souveraineté des données de santé et visent à garantir le respect du RGPD (le précédent référentiel ayant été approuvé avant l'entrée en vigueur du RGPD).

Le dispositif de certification HDS doit apporter des garanties aux acteurs du secteur sanitaire et médico-social quant à la protection des données vis-à-vis des législations extracommunautaires qui pourraient présenter un risque de divulgation de données et ne pas apporter de garanties aux personnes quant à l'effectivité des droits qui leur sont reconnus par le règlement général sur la protection des données (RGPD).

Le référentiel a fait l'objet d'un avis de l'autorité de protection des données française (CNIL) en date du 13 juillet 2023.

Dans l'attente de l'aboutissement des discussions au niveau européen sur les futurs référentiels européens (EUCS – European Cybersecurity Certification Scheme for Cloud services), le choix a été fait de ne pas s'aligner, à date, sur les exigences en termes d'immunité extra-territoriale prévues par le référentiel français dit "SecNumCloud version 3.2", adopté par l'ANSSI (agence française de sécurité des systèmes d'information).

10. Références aux textes de référence: 2017/0343/F,2017/0379/F

Les textes de référence doivent être envoyés dans le cadre de précédente notification:
2017/0343/F
2017/0379/F

11. Non

12.

13. Non

14. Non

15. Non

16.
Aspect OTC: Non

Aspects SPS: Non

****
Commission européenne
Point de contact Directive (UE) 2015/1535
email: grow-dir2015-1535-central@ec.europa.eu