►**B**

DÉCISION D'EXÉCUTION (UE) 2019/1765 DE LA COMMISSION

du 22 octobre 2019

arrêtant les règles relatives à la création, à la gestion et au fonctionnement du réseau d'autorités nationales chargées de la santé en ligne, et abrogeant la décision d'exécution 2011/890/UE

[notifiée sous le numéro C(2019) 7460]

(Texte présentant de l'intérêt pour l'EEE)

(JO L 270 du 24.10.2019, p. 83)

Modifiée par:

		Journal officiel		
		n°	page	date
►**M1**	Décision d'exécution (UE) 2020/1023 de la Commission du 15 juillet 2020	L 227 I	1	16.7.2020

▼B

DÉCISION D'EXÉCUTION (UE) 2019/1765 DE LA COMMISSION

du 22 octobre 2019

arrêtant les règles relatives à la création, à la gestion et au fonctionnement du réseau d'autorités nationales chargées de la santé en ligne, et abrogeant la décision d'exécution 2011/890/UE

[notifiée sous le numéro C(2019) 7460]

(Texte présentant de l'intérêt pour l'EEE)

Article premier

Objet

La présente décision arrête les règles nécessaires à la création, à la gestion et au fonctionnement du réseau «Santé en ligne» des autorités nationales chargées de la santé en ligne, conformément à l'article 14 de la directive 2011/24/UE.

Article 2

Définitions

1. Aux fins de la présente décision, on entend par:

a) «réseau "Santé en ligne"», le réseau constitué sur la base du volontariat reliant les autorités nationales chargées de la santé en ligne désignées par les États membres et poursuivant les objectifs énoncés à l'article 14 de la directive 2011/24/UE;

b) «points de contact nationaux pour la santé en ligne», des passerelles organisationnelles et techniques pour la fourniture de services transfrontaliers d'information sur la santé en ligne relevant de la responsabilité des États membres;

c) «services transfrontaliers d'information sur la santé en ligne», les services existants qui sont traités par les points de contact nationaux pour la santé en ligne et par l'intermédiaire d'une plateforme de services centrale développée par la Commission aux fins des soins de santé transfrontaliers;

d) «infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne», l'infrastructure qui permet la fourniture de services transfrontaliers d'information sur la santé en ligne par l'intermédiaire des points de contact nationaux pour la santé en ligne et de la plateforme européenne de services centrale. Cette infrastructure comprend à la fois des services génériques, tels que définis à l'article 2, paragraphe 2, point e), du règlement (UE) n° 283/2014, développés par les États membres, et une plateforme de services centrale, telle que définie à l'article 2, paragraphe 2, point d), du même règlement, développée par la Commission;

e) «autres services européens de santé en ligne partagés», les services numériques susceptibles d'être développés dans le cadre du réseau «Santé en ligne» et partagés entre les États membres;

▼B

f) «modèle de gouvernance», un ensemble de règles relatives à la désignation d'organismes participant aux processus décisionnels concernant l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne ou d'autres services européens de santé en ligne partagés développés dans le cadre du réseau «Santé en ligne», ainsi que la description de ces processus;

▼M1

g) «utilisateur d'application», toute personne qui possède un appareil intelligent sur lequel elle a téléchargé et utilise une application mobile autorisée de suivi de contacts et d'alerte;

h) «suivi de contacts», les mesures appliquées en vue de rechercher les personnes qui ont été exposées à une source de menace transfrontière grave sur la santé au sens de l'article 3, point c), de la décision n° 1082/2013/UE du Parlement européen et du Conseil ([1]);

i) «application mobile nationale de suivi de contacts et d'alerte», une application informatique autorisée à l'échelle nationale et fonctionnant sur des appareils intelligents, en particulier sur des smartphones, destinée généralement à des interactions variées et ciblées avec des ressources web et qui traite des données de proximité et d'autres informations contextuelles recueillies par de nombreux capteurs installés dans les appareils intelligents afin d'assurer le suivi des contacts avec les personnes infectées par le SARS-CoV-2 et d'avertir les personnes susceptibles d'avoir été exposées à ce virus. Ces applications mobiles peuvent détecter la présence d'autres appareils utilisant la technologie Bluetooth et échanger des informations avec les serveurs d'arrière-plan au moyen de l'internet;

j) «plateforme de fédération», une passerelle de réseau gérée par la Commission par l'intermédiaire d'un outil informatique sécurisé qui reçoit, enregistre et met à disposition un ensemble minimal de données à caractère personnel entre les serveurs d'arrière-plan des États membres dans le but d'assurer l'interopérabilité des applications mobiles nationales de suivi de contacts et d'alerte;

k) «clé», un identifiant éphémère unique lié à un utilisateur d'application qui déclare avoir été infecté par le SARS-CoV-2 ou qui est susceptible d'avoir été exposé à ce virus;

l) «vérification de l'infection», la méthode employée pour confirmer une infection par le SARS-CoV-2, selon que cette infection a été déclarée par l'utilisateur d'application concerné ou qu'elle a été confirmée par une autorité sanitaire nationale ou un test en laboratoire;

m) «pays concerné(s)», le ou les État(s) membre(s) dans le(s)quel(s) un utilisateur d'application se trouvait au cours des 14 jours précédant la date de téléchargement des clés et dans le(s)quel(s) cet utilisateur a téléchargé l'application mobile nationale autorisée de suivi de contacts et d'alerte et/ou a voyagé;

([1]) Décision n° 1082/2013/UE du Parlement européen et du Conseil du 22 octobre 2013 relative aux menaces transfrontières graves sur la santé et abrogeant la décision n° 2119/98/CE (JO L 293 du 5.11.2013, p. 1).

▼M1

n) «pays d'origine des clés», l'État membre dans lequel se trouve le serveur d'arrière-plan qui a téléchargé les clés sur la plateforme de fédération;

o) «données de journal», l'enregistrement automatique d'une activité liée à l'échange de données traitées par l'intermédiaire du portail de fédération ainsi qu'à l'accès à de telles données, qui indique notamment le type de l'activité de traitement effectuée, la date et l'heure de cette activité, ainsi que l'identifiant de la personne qui a procédé au traitement des données.

▼B

2. Les définitions figurant à l'article 4, points 1), 2), 7) et 8), du règlement (UE) 2016/679 s'appliquent en conséquence.

Article 3

Adhésion au réseau «Santé en ligne»

1. Les membres du réseau «Santé en ligne» sont les autorités des États membres chargées de la santé en ligne, désignées par les États membres participant au réseau «Santé en ligne».

2. Les États membres souhaitant participer au réseau «Santé en ligne» notifient par écrit à la Commission:

a) leur décision de participer au réseau «Santé en ligne»;

b) l'autorité nationale chargée de la santé en ligne qui deviendra membre du réseau «Santé en ligne», ainsi que le nom du représentant et celui de son suppléant.

3. Les membres notifient à la Commission les éléments suivants par écrit:

a) leur décision de se retirer du réseau «Santé en ligne»;

b) tout changement dans les informations visées au paragraphe 2, point b).

4. La Commission met à la disposition du public la liste des membres participant au réseau «Santé en ligne».

Article 4

Activités du réseau «Santé en ligne»

1. Dans la poursuite de l'objectif visé à l'article 14, paragraphe 2, point a), de la directive 2011/24/UE, le réseau «Santé en ligne» peut notamment:

a) promouvoir une plus grande interopérabilité des systèmes nationaux de technologies de l'information et de la communication et la transférabilité transfrontalière des données électroniques de santé dans le cadre des soins de santé transfrontaliers;

b) fournir des orientations aux États membres, en coopération avec d'autres autorités de contrôle compétentes, en ce qui concerne le partage des données de santé entre les États membres et le fait de mettre les citoyens en mesure d'accéder à leurs propres données de santé et de les partager;

▼B

c) fournir des orientations aux États membres et faciliter l'échange de bonnes pratiques en ce qui concerne la mise au point de différents services de santé numérique, tels que la télémédecine, la santé mobile ou les nouvelles technologies dans le domaine des mégadonnées et de l'intelligence artificielle, en prenant en considération les actions en cours au niveau de l'Union européenne;

d) fournir des orientations aux États membres en ce qui concerne la promotion de la santé, la prévention des maladies et l'amélioration de la fourniture des soins de santé grâce à une meilleure utilisation des données de santé et à l'amélioration des compétences numériques des patients et des professionnels de la santé;

e) fournir des orientations aux États membres et faciliter l'échange volontaire de bonnes pratiques sur les investissements dans les infrastructures numériques;

f) fournir aux États membres, en collaboration avec les autres organismes et parties prenantes concernés, des orientations sur les cas d'utilisation nécessaires à des fins d'interopérabilité clinique et sur les outils pertinents dans ce cadre;

g) fournir des orientations aux membres sur la sécurité de l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne ou d'autres services européens de santé en ligne partagés développés dans le cadre du réseau «Santé en ligne», en prenant en considération la législation et les documents élaborés au niveau de l'Union, notamment dans le domaine de la sécurité, ainsi que les recommandations dans le domaine de la cybersécurité, en étroite collaboration avec le groupe de coopération sur la sécurité des réseaux et de l'information et avec l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information, de même qu'avec les autorités nationales, le cas échéant;

▼M1

h) fournir des orientations aux États membres en ce qui concerne l'échange transfrontière de données à caractère personnel entre les applications mobiles nationales de suivi de contacts et d'alerte par l'intermédiaire de la plateforme de fédération.

▼B

2. Dans le cadre de l'élaboration des orientations concernant des méthodes concrètes permettant d'utiliser les données médicales à des fins de santé publique et de recherche visées à l'article 14, paragraphe 2, point b) ii), de la directive 2011/24/UE, le réseau «Santé en ligne» tient compte des lignes directrices adoptées par le comité européen de la protection des données et, le cas échéant, se concerte avec celui-ci. Ces orientations peuvent également porter sur les informations échangées dans le cadre de l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne ou d'autres services européens de santé en ligne partagés.

Article 5

Fonctionnement du réseau «Santé en ligne»

1. Le réseau «Santé en ligne» adopte son propre règlement intérieur à la majorité simple de ses membres.

2. Le réseau «Santé en ligne» adopte un programme de travail pluriannuel et un instrument d'évaluation pour la mise en œuvre de celui-ci.

▼B

3. Pour mener à bien ses missions, le réseau «Santé en ligne» peut créer des sous-groupes permanents en rapport avec des tâches spécifiques, notamment en ce qui concerne l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne ou les autres services européens de santé en ligne partagés développés dans le cadre du réseau «Santé en ligne».

4. Le réseau «Santé en ligne» peut aussi mettre en place des sous-groupes temporaires, y compris en collaboration avec des experts, pour l'examen de questions particulières sur la base d'un mandat qu'il définit lui-même. Ces sous-groupes sont dissous aussitôt leur mandat rempli.

5. Lorsque des membres du réseau «Santé en ligne» décident d'approfondir leur coopération dans certains domaines couverts par les missions du réseau, ils devraient s'accorder sur les règles de cette coopération approfondie et s'engager à les respecter.

6. Dans la poursuite de ses objectifs, le réseau «Santé en ligne» travaille en coopération étroite avec les actions conjointes qui appuient les activités du réseau «Santé en ligne», lorsque de telles actions conjointes existent, avec les parties prenantes ou avec les autres organes ou mécanismes d'appui concernés et prend en considération les résultats obtenus dans le cadre de ces activités.

7. Le réseau «Santé en ligne» développe, conjointement avec la Commission, les modèles de gouvernance de l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne et participe à cette gouvernance:

i) en s'accordant sur les priorités de l'infrastructure de services numériques dans le domaine de la santé en ligne et en supervisant leur mise en œuvre;

ii) en élaborant des orientations et des exigences pour la mise en œuvre, y compris la sélection des normes utilisées pour l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne;

iii) en s'accordant sur la question de savoir si les membres du réseau «Santé en ligne» doivent être autorisés ou non à commencer et à continuer à échanger des données électroniques de santé au moyen de l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne, par l'intermédiaire de leurs points de contact nationaux pour la santé en ligne, en fonction de leur conformité avec les exigences établies par le réseau «Santé en ligne», telle qu'évaluée dans le cadre des essais fournis par la Commission et des audits réalisés par celle-ci;

iv) en approuvant le plan de travail annuel relatif à l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne.

8. Le réseau «Santé en ligne» peut développer, conjointement avec la Commission, les modèles de gouvernance d'autres services européens de santé en ligne partagés mis au point dans le cadre du réseau «Santé en ligne» et participer à leur gouvernance. Le réseau peut également définir les priorités, conjointement avec la Commission, et élaborer des orientations concernant le fonctionnement de ces services européens de santé en ligne partagés.

▼B

9. Le règlement intérieur peut prévoir que des pays autres que les États membres, appliquant la directive 2011/24/UE, peuvent participer aux réunions du réseau «Santé en ligne» en tant qu'observateurs.

10. Les membres du réseau «Santé en ligne» et leurs représentants, ainsi que les experts et observateurs invités, respectent les obligations de secret professionnel prévues à l'article 339 du traité, ainsi que les règles de sécurité de la Commission concernant la protection des informations classifiées de l'Union européenne, définies dans la décision (UE, Euratom) 2015/444 de la Commission ([1]). En cas de non-respect de ces obligations, le président du réseau «Santé en ligne» peut prendre toutes les mesures appropriées prévues dans le règlement intérieur.

Article 6

Relation entre le réseau «Santé en ligne» et la Commission

1. La Commission:

a) assiste aux réunions du réseau «Santé en ligne», dont elle assume la coprésidence, conjointement avec le représentant des membres;

b) coopère avec le réseau «Santé en ligne» et lui fournit un soutien en ce qui concerne ses activités;

c) assure le secrétariat du réseau «Santé en ligne»;

d) élabore, met en œuvre et tient à jour des mesures techniques et organisationnelles appropriées liées aux services centraux de l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne;

e) aide le réseau «Santé en ligne» à s'accorder sur la conformité technique et organisationnelle des points de contact nationaux pour la santé en ligne avec les exigences en matière d'échange transfrontalier de données de santé, en fournissant et en réalisant les essais et les audits nécessaires. Des experts des États membres peuvent assister les auditeurs de la Commission;

▼M1

f) élabore, met en œuvre et tient à jour des mesures techniques et organisationnelles appropriées liées à la sécurité de la transmission et de l'hébergement de données à caractère personnel sur la plateforme de fédération en vue d'assurer l'interopérabilité des applications mobiles nationales de suivi de contacts et d'alerte;

g) aide le réseau «Santé en ligne» à s'accorder sur la conformité technique et organisationnelle des autorités nationales avec les exigences en matière d'échange transfrontière de données à caractère personnel sur la plateforme de fédération, en fournissant et en réalisant les essais et les audits nécessaires. Des experts des États membres peuvent assister les auditeurs de la Commission.

▼B

2. La Commission peut assister aux réunions des sous-groupes du réseau «Santé en ligne».

3. La Commission peut consulter le réseau «Santé en ligne» sur les questions liées à la santé en ligne au niveau de l'Union et à l'échange de bonnes pratiques en matière de santé en ligne.

([1]) Décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 72 du 17.3.2015, p. 53).

▼B

4. La Commission met à la disposition du public les informations relatives aux activités menées par le réseau «Santé en ligne».

Article 7

▼M1

Protection des données à caractère personnel traitées par l'intermédiaire de l'infrastructure de services numériques dans le domaine de la santé en ligne

▼B

1. Les États membres, représentés par les autorités nationales compétentes ou d'autres organismes désignés, sont considérés comme des responsables du traitement des données à caractère personnel qu'ils traitent dans le cadre de l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne et ils répartissent de manière claire et transparente les responsabilités entre les responsables du traitement des données.

2. La Commission est considérée comme sous-traitant pour les données à caractère personnel des patients traitées dans le cadre de l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne. En sa qualité de sous-traitant, la Commission gère les services centraux de l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne et respecte les obligations qui incombent aux sous-traitants, énoncées à l'►M1 annexe I ◄ de la présente décision. La Commission n'a pas accès aux données à caractère personnel des patients traitées dans le cadre de l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne.

3. La Commission est considérée comme responsable du traitement des données à caractère personnel nécessaires pour accorder et gérer les droits d'accès aux services centraux de l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne. Ces données sont les coordonnées des utilisateurs, y compris leurs prénom, nom, leur adresse électronique et leur appartenance.

▼M1

Article 7 bis

Échange transfrontière de données entre les applications mobiles nationales de suivi de contacts et d'alerte par l'intermédiaire de la plateforme de fédération

1. Lorsque des données à caractère personnel sont échangées au moyen de la plateforme de fédération, leur traitement est limité aux finalités consistant à faciliter l'interopérabilité des applications mobiles nationales de suivi de contacts et d'alerte dans le cadre de la plateforme de fédération ainsi qu'à assurer la continuité du suivi des contacts dans un contexte transfrontière.

2. Les données à caractère personnel visées au paragraphe 3 sont transmises à la plateforme de fédération sous une forme pseudonymisée.

▼M1

3. Les données à caractère personnel pseudonymisées échangées via la plateforme de fédération et traitées dans ce cadre renferment uniquement les informations suivantes:

a) les clés transmises par les applications mobiles nationales de suivi de contacts et d'alerte au maximum 14 jours avant la date de téléchargement des clés;

b) les données de journal associées aux clés conformément au protocole de spécifications techniques utilisé dans le pays d'origine de ces clés;

c) la vérification de l'infection;

d) les pays concernés et le pays d'origine des clés.

4. Les autorités nationales ou organismes officiels désigné(e)s qui traitent les données à caractère personnel sur la plateforme de fédération sont responsables conjoints du traitement des données effectué dans ce cadre. Les responsabilités respectives des responsables conjoints du traitement sont réparties conformément à l'annexe II. Tout État membre qui souhaite participer à l'échange transfrontière de données entre les applications mobiles nationales de suivi de contacts et d'alerte en informe la Commission avant de se joindre à cette initiative et indique l'autorité nationale ou l'organisme officiel qui a été désigné(e) comme responsable du traitement.

5. La Commission endosse le rôle de sous-traitant des données à caractère personnel traitées dans le cadre de la plateforme de fédération. En sa qualité de sous-traitant, la Commission veille à la sécurité du traitement, y compris la transmission et l'hébergement, des données à caractère personnel dans le cadre de la plateforme de fédération et s'acquitte des obligations incombant aux sous-traitants énoncées à l'annexe III.

6. L'efficacité des mesures techniques et organisationnelles visant à garantir la sécurité du traitement des données à caractère personnel sur la plateforme de fédération est régulièrement testée, analysée et évaluée par la Commission et les autorités nationales autorisées à avoir accès à cette plateforme.

7. Sans préjudice de la décision des responsables conjoints du traitement de mettre un terme au traitement dans le cadre de la plateforme de fédération, cette dernière est désactivée au plus tard 14 jours après que toutes les applications mobiles nationales de suivi de contacts et d'alerte connectées ont cessé de transmettre des clés par l'intermédiaire de cette plateforme.

▼B

Article 8

Frais

1. Les participants aux activités du réseau «Santé en ligne» ne sont pas rémunérés par la Commission pour leurs services.

▼B

2. Les frais de déplacement et de séjour des participants aux activités du réseau «Santé en ligne» sont remboursés par la Commission conformément aux dispositions en vigueur à la Commission relatives à l'indemnisation des personnes étrangères à la Commission convoquées en qualité d'expert. Ces frais sont remboursés dans la limite des crédits disponibles alloués dans le cadre de la procédure annuelle d'allocation des ressources.

Article 9

Abrogation

La décision d'exécution 2011/890/UE est abrogée. Les références à la décision abrogée s'entendent comme faites à la présente décision.

Article 10

Destinataires

Les États membres sont destinataires de la présente décision.

▼M1

ANNEXE I

▼B

RESPONSABILITÉS DE LA COMMISSION EN TANT QUE SOUS-TRAITANT DES DONNÉES DANS LE CADRE DE L'INFRASTRUCTURE DE SERVICES NUMÉRIQUES DANS LE DOMAINE DE LA SANTÉ EN LIGNE POUR LES SERVICES TRANSFRONTALIERS D'INFORMATION SUR LA SANTÉ EN LIGNE

La Commission:

1. Met en place et garantit une infrastructure de communication sécurisée et fiable qui assure l'interconnexion entre les réseaux des membres du réseau «Santé en ligne» participant à l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne (l'«infrastructure de communication sécurisée centrale»). Afin de remplir ces obligations, la Commission peut engager des tiers. La Commission veille à ce que les mêmes obligations en matière de protection des données que celles énoncées dans la présente décision s'appliquent à ces tiers.

2. Configure une partie de l'infrastructure de communication sécurisée centrale de telle sorte que les points de contact nationaux pour la santé en ligne puissent échanger des informations de manière sécurisée, fiable et efficace.

3. Traite les données personnelles selon des instructions documentées fournies par les responsables du traitement des données.

4. Prend toutes les mesures de sécurité nécessaires sur les plans organisationnel, physique et logique pour maintenir l'infrastructure de communication sécurisée centrale. À cette fin, la Commission:

   a) désigne une entité responsable de la gestion de la sécurité au niveau de l'infrastructure de communication sécurisée centrale, communique ses coordonnées aux responsables du traitement des données et veille à sa disponibilité pour répondre aux menaces pour la sécurité;

   b) assume la responsabilité de la sécurité de l'infrastructure de communication sécurisée centrale;

   c) veille à ce que toutes les personnes qui se voient accorder l'accès à l'infrastructure de communication sécurisée centrale soient soumises à une obligation contractuelle, professionnelle ou statutaire de confidentialité;

   d) veille à ce que le personnel ayant accès aux informations classifiées réponde aux critères correspondants en matière d'habilitation et de confidentialité.

5. Prend toutes les mesures de sécurité nécessaires pour éviter de compromettre le bon fonctionnement opérationnel du domaine des autres. À cette fin, la Commission met en place les procédures spécifiques relatives à la connexion à l'infrastructure de communication sécurisée centrale. Ces procédures comprennent:

   a) une procédure d'évaluation des risques, afin d'identifier et d'estimer les menaces potentielles pour le système;

   b) une procédure d'audit et de contrôle destinée à:

      i) vérifier la correspondance entre les mesures de sécurité mises en œuvre et la politique de sécurité appliquée;

      ii) contrôler régulièrement l'intégrité des fichiers système, les paramètres de sécurité et les autorisations accordées;

      iii) assurer une surveillance afin de détecter les atteintes à la sécurité et les intrusions;

      iv) appliquer des modifications afin d'éviter les failles existantes en matière de sécurité;

▼B

v) définir les conditions d'autorisation, y compris à la demande des responsables du traitement, et contribuer à la réalisation d'audits indépendants, y compris des inspections, et d'examens des mesures de sécurité;

c) une procédure de contrôle des modifications afin de documenter et de mesurer l'incidence des modifications avant leur mise en œuvre et de tenir les points de contact nationaux pour la santé en ligne informés de toute modification susceptible d'affecter la communication avec les autres infrastructures nationales et/ou leur sécurité;

d) une procédure de maintenance et de réparation afin de préciser les règles et les conditions à respecter lors de la maintenance et/ou de la réparation des équipements;

e) une procédure relative aux incidents de sécurité afin de définir le système de signalement et d'escalade, d'informer sans délai l'administration nationale responsable, ainsi que le contrôleur européen de la protection des données de toute atteinte à la sécurité et de définir une procédure disciplinaire pour traiter les atteintes à la sécurité.

6. Prend des mesures de sécurité physiques et/ou logiques pour les installations hébergeant l'équipement de l'infrastructure de communication sécurisée centrale ainsi que pour les contrôles d'accès de sécurité et les contrôles d'accès aux données logiques. À cette fin, la Commission:

a) assure la sécurité physique afin de mettre en place des périmètres de sécurité caractéristiques et de permettre la détection des atteintes;

b) contrôle l'accès aux installations et tient un registre des visiteurs à des fins de traçage;

c) veille à ce que les personnes extérieures auxquelles l'accès est accordé soient accompagnées par du personnel dûment autorisé de leur organisation;

d) veille à ce que des équipements ne puissent être ajoutés, remplacés ou retirés sans autorisation préalable des organismes compétents désignés;

e) contrôle l'accès depuis et vers d'autres réseaux interconnectés avec l'infrastructure de communication sécurisée centrale;

f) veille à ce que les personnes qui accèdent à l'infrastructure de communication sécurisée centrale soient identifiées et authentifiées;

g) réexamine les droits d'autorisation liés à l'accès à l'infrastructure de communication sécurisée centrale en cas d'atteinte à la sécurité touchant cette infrastructure;

h) préserve l'intégrité des informations transmises dans le cadre de l'infrastructure de communication sécurisée centrale;

i) met en œuvre des mesures de sécurité d'ordre technique et organisationnel afin d'empêcher l'accès non autorisé aux données à caractère personnel;

j) met en œuvre, en tant que de besoin, des mesures visant à empêcher tout accès non autorisé à l'infrastructure de communication sécurisée centrale depuis le domaine des points de contact nationaux pour la santé en ligne (c'est-à-dire: blocage d'une localisation/d'une adresse IP).

7. Prend des mesures pour protéger son domaine, y compris la rupture des connexions, en cas d'écart important par rapport aux principes et concepts de qualité ou de sécurité.

8. Maintient un plan de gestion des risques lié à son domaine de compétence.

▼B

9. Surveille — en temps réel — la performance de tous les éléments de service des services de son infrastructure de communication sécurisée centrale, produit des statistiques régulières et tient des registres.

10. Fournit un soutien à tous les services de l'infrastructure de communication sécurisée centrale en anglais, 24 h sur 24 et 7 j sur 7, par téléphone, courrier ou portail web et accepte les appels émanant d'appelants autorisés: les coordonnateurs de l'infrastructure de communication sécurisée centrale et leurs services d'assistance respectifs, les responsables de projets et les personnes désignées de la Commission.

11. Soutient les responsables du traitement des données en fournissant des informations sur l'infrastructure de communication sécurisée centrale de l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne, dans le but de mettre en application les obligations énoncées aux articles 35 et 36 du règlement (UE) 2016/679.

12. Veille à ce que les données transportées au sein de l'infrastructure de communication sécurisée centrale soient chiffrées.

13. Prend toutes les mesures appropriées pour empêcher que les opérateurs de l'infrastructure de communication sécurisée centrale disposent d'un accès non autorisé aux données transportées.

14. Prend des mesures pour faciliter l'interopérabilité et la communication entre les administrations nationales compétentes désignées de l'infrastructure de communication sécurisée centrale.

▼M1

ANNEXE II

RESPONSABILITÉS DES ÉTATS MEMBRES PARTICIPANTS EN TANT QUE RESPONSABLES CONJOINTS DU TRAITEMENT DANS LE CADRE DE LA PLATEFORME DE FÉDÉRATION EN CE QUI CONCERNE LE TRAITEMENT TRANSFRONTIÈRE ENTRE LES APPLICATIONS MOBILES NATIONALES DE SUIVI DE CONTACTS ET D'ALERTE

SECTION 1

Sous-section 1

Répartition des responsabilités

1. Les responsables conjoints du traitement traitent les données à caractère personnel par l'intermédiaire de la plateforme de fédération conformément aux spécifications techniques définies par le réseau «Santé en ligne» ([1]).

2. Il incombe à chaque responsable du traitement de traiter les données à caractère personnel dans le cadre de la plateforme de fédération conformément au règlement général sur la protection des données et à la directive 2002/58/CE.

3. Chaque responsable du traitement met en place un point de contact doté d'une boîte aux lettres fonctionnelle qui servira à la communication entre les responsables conjoints du traitement, ainsi qu'entre ces derniers et le sous-traitant.

4. Un sous-groupe temporaire mis en place par le réseau «Santé en ligne» conformément à l'article 5, paragraphe 4, est chargé d'examiner toute question relative à l'interopérabilité des applications mobiles nationales de suivi de contacts et d'alerte et à la responsabilité conjointe du traitement de données à caractère personnel correspondant, ainsi que de faciliter la communication d'instructions coordonnées à la Commission en tant que sous-traitant. Dans le cadre du sous-groupe temporaire, les responsables du traitement peuvent notamment œuvrer à une approche commune en matière de conservation des données dans leurs serveurs d'arrière-plan nationaux, compte tenu de la période de conservation fixée dans le portail de fédération.

5. Les instructions à l'intention du sous-traitant sont envoyées par le point de contact de l'un des responsables conjoints du traitement, en accord avec les autres responsables conjoints du traitement faisant partie du sous-groupe mentionné ci-dessus.

6. Seules les personnes autorisées par les autorités nationales ou les organismes officiels désigné(e)s peuvent accéder aux données à caractère personnel des utilisateurs échangées dans le cadre de la plateforme de fédération.

7. Chaque autorité nationale ou organisme officiel désigné(e) perd sa qualité de responsable conjoint du traitement à compter de la date de son renoncement à participer à la plateforme de fédération. L'entité concernée reste toutefois responsable des traitements de données effectués dans le cadre de la plateforme de fédération avant qu'elle ne s'en retire.

Sous-section 2

Responsabilités et rôles en matière de traitement des demandes et d'information des personnes concernées

1. Chaque responsable du traitement fournit aux utilisateurs de son application mobile nationale de suivi de contacts et d'alerte (ci-après es «personnes concernées») des informations sur le traitement de leurs données à lcaractère

([1]) En particulier, les spécifications en matière d'interopérabilité applicables aux chaînes de transmission transfrontières entre applications approuvées, du 16 juin 2020, disponibles à l'adresse suivante: https://ec.europa.eu/health/ehealth/key_documents_fr#anchor0

▼M1

personnel dans le cadre de la plateforme de fédération aux fins de l'interopérabilité transfrontière des applications mobiles nationales de suivi de contacts et d'alerte, conformément aux articles 13 et 14 du règlement général sur la protection des données.

2. Chaque responsable du traitement fait office de point de contact pour les utilisateurs de son application mobile nationale de suivi de contacts et d'alerte et traite les demandes présentées par ces utilisateurs ou par leurs représentants relatives à l'exercice des droits des personnes concernées conformément au règlement général sur la protection des données. Chaque responsable du traitement désigne un point de contact spécifique pour les demandes reçues des personnes concernées. Si un responsable conjoint du traitement reçoit une demande d'une personne concernée qui ne relève pas de sa responsabilité, il la transmet rapidement au responsable conjoint du traitement compétent. Sur demande, les responsables conjoints du traitement se prêtent mutuellement assistance pour le traitement des demandes des personnes concernées et se répondent dans les meilleurs délais, et au plus tard dans les 15 jours qui suivent la réception d'une demande d'assistance.

3. Chaque responsable du traitement porte à la connaissance des personnes concernées le contenu de la présente annexe, notamment les modalités prévues aux points 1) et 2).

SECTION 2

Gestion des incidents de sécurité, notamment des violations de données à caractère personnel

1. Les responsables conjoints du traitement se prêtent mutuellement assistance pour la détection et la gestion des incidents de sécurité, notamment des violations de données à caractère personnel, en lien avec le traitement de données dans le cadre de la plateforme de fédération.

2. En particulier, les responsables conjoints du traitement s'informent mutuellement des éléments suivants:

   a) tout risque potentiel ou avéré pour la disponibilité, la confidentialité et/ou l'intégrité des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la plateforme de fédération;

   b) tout incident de sécurité lié au processus de traitement dans le cadre de la plateforme de fédération;

   c) toute violation de données à caractère personnel, les conséquences probables de ladite violation et l'évaluation du risque pour les droits et libertés des personnes physiques, ainsi que toute mesure prise visant à remédier à la violation de données à caractère personnel et à atténuer le risque pour les droits et libertés des personnes physiques;

   d) toute atteinte aux garanties techniques et/ou organisationnelles du processus de traitement dans le cadre de la plateforme de fédération.

3. Les responsables conjoints du traitement communiquent toute violation de données à caractère personnel liée au processus de traitement dans le cadre de la plateforme de fédération à la Commission, aux autorités de contrôle compétentes et, lorsqu'ils sont tenus de le faire, aux personnes concernées, conformément aux articles 33 et 34 du règlement (UE) 2016/679 ou à la suite d'une notification par la Commission.

SECTION 3

Analyse d'impact relative à la protection des données

1. Si, afin de s'acquitter des obligations qui lui incombent en vertu des articles 35 et 36 du règlement général sur la protection des données, un responsable du traitement a besoin de s'informer auprès d'un autre responsable du traitement, il adresse une demande spécifique à la boîte aux lettres fonctionnelle visée à la section 1, sous-section 1, point 3). L'autre responsable du traitement met tout en œuvre pour fournir les informations demandées.

▼M1

ANNEXE III

RESPONSABILITÉS DE LA COMMISSION EN TANT QUE SOUS-TRAITANT DES DONNÉES DANS LE CADRE DE LA PLATEFORME DE FÉDÉRATION EN CE QUI CONCERNE LE TRAITEMENT TRANSFRONTIÈRE ENTRE LES APPLICATIONS MOBILES NATIONALES DE SUIVI DE CONTACTS ET D'ALERTE

Les responsabilités de la Commission sont définies ci-dessous.

1) La Commission met en place et garantit une infrastructure de communication sécurisée et fiable qui assure l'interconnexion des applications mobiles nationales de suivi de contacts et d'alerte des États membres participant à la plateforme de fédération. Afin de s'acquitter de ses obligations en tant que sous-traitant des données de la plateforme de fédération, la Commission peut faire appel à des tiers comme sous-traitants ultérieurs; la Commission informe les responsables conjoints du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants ultérieurs, donnant ainsi aux responsables du traitement la possibilité d'émettre conjointement des objections à l'encontre de ces changements conformément à l'annexe II, section 1, sous-section 1, point 4). La Commission veille à ce que les mêmes obligations en matière de protection des données que celles énoncées dans la présente décision s'appliquent à ces sous-traitants ultérieurs.

2) La Commission ne traite les données à caractère personnel que sur instruction documentée des responsables du traitement, à moins qu'elle ne soit tenue d'y procéder en vertu du droit de l'Union ou du droit d'un État membre; dans ce cas, la Commission informe les responsables du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit la communication d'une telle information pour des motifs importants d'intérêt public.

3) Le traitement par la Commission comporte les éléments suivants:

   a) l'authentification des serveurs d'arrière-plan nationaux, fondée sur les certificats des serveurs d'arrière-plan nationaux;

   b) la réception des données visées à l'article 7 *bis*, paragraphe 3, de la décision d'exécution téléchargées par les serveurs d'arrière-plan nationaux à l'aide d'une interface de programmation d'application mise à disposition, qui permet aux serveurs d'arrière-plan nationaux de télécharger les données pertinentes;

   c) le stockage des données dans la plateforme de fédération dès leur réception à partir des serveurs d'arrière-plan nationaux;

   d) la mise à disposition des données aux fins de leur téléchargement par les serveurs d'arrière-plan nationaux;

   e) la suppression des données une fois téléchargées par tous les serveurs d'arrière-plan participants ou 14 jours après leur réception, selon ce qui se produit en premier;

   f) après la fin de la prestation de service, la suppression de toutes les données restantes, à moins que le stockage des données à caractère personnel ne soit exigé au titre du droit de l'Union ou du droit d'un État membre.

   Le sous-traitant prend les mesures nécessaires pour préserver l'intégrité des données traitées.

4) La Commission prend toutes les mesures de sécurité à la pointe de la technique nécessaires sur les plans organisationnel, physique et logique pour maintenir la plateforme de fédération. À cette fin, la Commission:

▼M1

a) désigne une entité responsable de la gestion de la sécurité au niveau de la plateforme de fédération, communique ses coordonnées aux responsables du traitement et veille à sa disponibilité pour répondre aux menaces pour la sécurité;

b) assume la responsabilité de la sécurité de la plateforme de fédération;

c) veille à ce que toutes les personnes qui se voient accorder l'accès à la plateforme de fédération soient soumises à une obligation contractuelle, professionnelle ou statutaire de confidentialité.

5) La Commission prend toutes les mesures de sécurité nécessaires pour éviter de compromettre le bon fonctionnement opérationnel des serveurs d'arrière-plan nationaux. À cette fin, la Commission met en place des procédures spécifiques relatives à la connexion à partir des serveurs d'arrière-plan à la plateforme de fédération. Ces procédures comprennent:

a) une procédure d'évaluation des risques, afin d'identifier et d'estimer les menaces potentielles pour le système;

b) une procédure d'audit et de contrôle destinée à:

i) vérifier la correspondance entre les mesures de sécurité mises en œuvre et la politique de sécurité applicable,

ii) contrôler régulièrement l'intégrité des fichiers système, les paramètres de sécurité et les autorisations accordées,

iii) assurer une surveillance afin de détecter les atteintes à la sécurité et les intrusions,

iv) appliquer des modifications afin de corriger les failles existantes en matière de sécurité,

v) permettre, y compris à la demande des responsables du traitement, la réalisation d'audits indépendants, y compris des inspections, et d'examens des mesures de sécurité, et y contribuer, sous réserve de conditions qui respectent le protocole n° 7 du traité sur le fonctionnement de l'Union européenne sur les privilèges et immunités de l'Union européenne ([1]);

c) une modification de la procédure de contrôle afin de documenter et de mesurer l'incidence des modifications avant leur mise en œuvre et de tenir les responsables du traitement informés de toute modification susceptible d'affecter la communication avec leurs infrastructures et/ou la sécurité de celles-ci;

d) une procédure de maintenance et de réparation afin de préciser les règles et les conditions à respecter lors de la maintenance et/ou de la réparation des équipements;

e) une procédure relative aux incidents de sécurité afin de définir le système de signalement et d'escalade, d'informer sans délai les responsables du traitement, ainsi que le Contrôleur européen de la protection des données, de toute violation des données à caractère personnel et de définir une procédure disciplinaire pour traiter les atteintes à la sécurité.

6) La Commission prend des mesures de sécurité physiques et/ou logiques à la pointe de la technique pour les installations hébergeant l'équipement de la plateforme de fédération ainsi que pour les contrôles d'accès de sécurité et les contrôles d'accès aux données logiques. À cette fin, la Commission:

([1]) Protocole (no 7) sur les privilèges et immunités de l'Union européenne (JO C 326 du 26.10.2012, p. 266).

▼**M1**

a) assure la sécurité physique afin de mettre en place des périmètres de sécurité distincts et de permettre la détection des atteintes;

b) contrôle l'accès aux installations et tient un registre des visiteurs à des fins de suivi;

c) veille à ce que les personnes extérieures auxquelles l'accès est accordé soient accompagnées par du personnel dûment autorisé;

d) veille à ce que des équipements ne puissent être ajoutés, remplacés ou retirés sans autorisation préalable des organismes compétents désignés;

e) contrôle l'accès à la plateforme de fédération depuis les serveurs d'arrière-plan nationaux et l'accès depuis la plateforme de fédération vers ceux-ci;

f) veille à ce que les personnes qui accèdent à la plateforme de fédération soient identifiées et authentifiées;

g) réexamine les droits d'autorisation liés à l'accès à la plateforme de fédération en cas d'atteinte à la sécurité touchant cette infrastructure;

h) préserve l'intégrité des informations transmises par l'intermédiaire de la plateforme de fédération;

i) met en œuvre des mesures de sécurité d'ordre technique et organisationnel afin d'empêcher l'accès non autorisé aux données à caractère personnel;

j) met en œuvre, en tant que de besoin, des mesures visant à empêcher tout accès non autorisé à la plateforme de fédération depuis le domaine des autorités nationales (c'est-à-dire: blocage d'une localisation/d'une adresse IP).

7) La Commission prend des mesures pour protéger son domaine, y compris la rupture des connexions, en cas d'écart important par rapport aux principes et concepts de qualité ou de sécurité.

8) La Commission maintient un plan de gestion des risques lié à son domaine de compétence.

9) La Commission surveille — en temps réel — la performance de tous les éléments de service des services de sa plateforme de fédération, produit des statistiques régulières et tient des registres.

10) La Commission fournit un soutien à tous les services de la plateforme de fédération en anglais, 24 heures sur 24 et 7 jours sur 7, par téléphone, courrier ou portail web, et accepte les appels émanant d'appelants autorisés: les coordonnateurs de la plateforme de fédération et leurs services d'assistance respectifs, les responsables de projets et les personnes désignées de la Commission.

11) La Commission aide les responsables du traitement au moyen de mesures techniques et organisationnelles appropriées, dans la mesure du possible, à s'acquitter de l'obligation qui leur incombe de répondre aux demandes d'exercice des droits de la personne concernée prévus au chapitre III du règlement général sur la protection des données.

▼**M1**

12) La Commission soutient les responsables du traitement des données en fournissant des informations sur la plateforme de fédération, dans le but de mettre en application les obligations énoncées aux articles 32, 35 et 36 du règlement général sur la protection des données.

13) La Commission veille à ce que les données traitées dans le cadre de la plateforme de fédération soient inintelligibles pour toute personne non autorisée à y accéder.

14) La Commission prend toutes les mesures appropriées pour empêcher que les opérateurs de la plateforme de fédération disposent d'un accès non autorisé aux données transmises.

15) La Commission prend des mesures pour faciliter l'interopérabilité et la communication entre les responsables du traitement désignés de la plateforme de fédération.

16) La Commission tient un registre des activités de traitement effectuées pour le compte des responsables du traitement conformément à l'article 31, paragraphe 2, du règlement (UE) 2018/1725.