II

(Actes non législatifs)

DÉCISIONS

DÉCISION D'EXÉCUTION (UE) 2020/1023 DE LA COMMISSION

du 15 juillet 2020

modifiant la décision d'exécution (UE) 2019/1765 en ce qui concerne l'échange transfrontière de données entre les applications mobiles nationales de suivi de contacts et d'alerte dans le cadre de la lutte contre la pandémie de COVID-19

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

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu la directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers ([1]), et notamment son article 14, paragraphe 3,

considérant ce qui suit:

(1) L'Union est chargée, en vertu de l'article 14 de la directive 2011/24/UE, de soutenir et faciliter la coopération et l'échange d'informations entre les États membres dans le cadre d'un réseau constitué sur la base du volontariat reliant les autorités nationales chargées de la santé en ligne désignées par les États membres (ci-après le «réseau "Santé en ligne"»).

(2) La décision d'exécution (UE) 2019/1765 de la Commission ([2]) arrête les règles relatives à la création, à la gestion et au fonctionnement du réseau d'autorités nationales chargées de la santé en ligne. L'article 4 de cette décision confie au réseau «Santé en ligne» la tâche de 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.

(3) Face à la crise de santé publique déclenchée par la pandémie de COVID-19, plusieurs États membres ont conçu des applications mobiles qui facilitent le suivi des contacts et permettent d'alerter leurs utilisateurs en les invitant à prendre des mesures appropriées, comme un test ou l'auto-isolement, s'ils ont été potentiellement exposés au virus lors de contacts avec un autre utilisateur de l'application qui a déclaré avoir été testé positif. Ces applications s'appuient sur la technologie Bluetooth pour détecter les contacts rapprochés entre différents appareils. Étant donné que les restrictions relatives aux déplacements entre les États membres sont levées depuis juin 2020, il convient d'accroître l'interopérabilité des systèmes nationaux de technologies de l'information et de la communication entre les États membres dans le cadre du réseau «Santé en ligne», en mettant en place une infrastructure numérique qui assure l'interopérabilité entre les applications mobiles nationales de suivi de contacts et d'alerte.

([1]) JO L 88 du 4.4.2011, p. 45.

([2]) 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 (JO L 270 du 24.10.2019, p. 83).

(4) La Commission apporte son soutien aux États membres en ce qui concerne les applications mobiles susmentionnées. Le 8 avril 2020, la Commission a adopté une recommandation concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées (ci-après la «recommandation de la Commission») ([3]). Les États membres participant au réseau «Santé en ligne» ont adopté, avec l'appui de la Commission, une boîte à outils commune au niveau de l'Union pour les États membres concernant les applications mobiles destinées à faciliter le suivi des contacts ([4]), ainsi que des lignes directrices sur l'interopérabilité des applications mobiles de suivi de contacts autorisées dans l'Union européenne ([5]). Cette boîte à outils présente les exigences nationales relatives aux applications mobiles nationales de suivi de contacts et d'alerte, en soulignant notamment que ces applications devraient se fonder sur une utilisation volontaire, obtenir l'autorisation des autorités sanitaires nationales compétentes, protéger la vie privée des utilisateurs et être supprimées dès qu'elles ne seront plus nécessaires. À la suite des dernières évolutions de la crise de la COVID-19, la Commission ([6]) et le comité européen de la protection des données ([7]) ont tous deux publié des orientations relatives à la protection des données dans le cadre des applications mobiles et des outils de suivi de contacts. La conception des applications mobiles des États membres et de l'infrastructure numérique destinée à assurer leur interopérabilité se fonde à la fois sur la boîte à outils commune au niveau de l'Union, sur les orientations mentionnées ci-dessus et sur les spécifications techniques définies au sein du réseau «Santé en ligne».

(5) Afin de favoriser l'interopérabilité des applications mobiles nationales de suivi de contacts et d'alerte, les États membres participant au réseau «Santé en ligne» qui avaient décidé de renforcer leur coopération dans ce domaine sur une base volontaire ont élaboré, avec l'aide de la Commission, une infrastructure numérique sous la forme d'un outil informatique d'échange de données. Cette infrastructure numérique a été baptisée «plateforme de fédération».

(6) La présente décision définit le rôle des États membres participants et de la Commission en ce qui concerne le fonctionnement de cette plateforme de fédération pour l'interopérabilité transfrontière des applications mobiles nationales de suivi de contacts et d'alerte.

(7) Le traitement des données à caractère personnel des utilisateurs d'applications mobiles de suivi de contacts et d'alerte, sous la responsabilité des États membres ou d'autres organisations publiques ou organismes officiels des États membres, devrait être effectué conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil ([8]) (ci-après le «règlement général sur la protection des données») et à la directive 2002/58/CE du Parlement européen et du Conseil ([9]). Le traitement des données à caractère personnel sous la responsabilité de la Commission en vue de gérer la plateforme de fédération et de garantir sa sécurité devrait respecter le règlement (UE) 2018/1725 du Parlement européen et du Conseil ([10]).

(8) La plateforme de fédération devrait prendre la forme d'une infrastructure informatique sécurisée présentant une interface commune, via laquelle les autorités nationales ou organismes officiels désigné(e)s pourront échanger un ensemble minimal de données concernant les contacts avec des personnes infectées par le SARS-CoV-2 afin d'informer d'autres personnes de leur exposition potentielle à cette infection, et favorisant une coopération efficace entre les États membres en matière de soins de santé en facilitant l'échange d'informations pertinentes.

(9) La présente décision devrait donc définir les modalités de l'échange transfrontière de données entre les autorités nationales ou organismes officiels désigné(e)s par l'intermédiaire de la plateforme de fédération au sein de l'Union européenne.

([3]) Recommandation (UE) 2020/518 de la Commission du 8 avril 2020 concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées (JO L 114 du 14.4.2020, p. 7).

([4]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

([5]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

([6]) Communication de la Commission intitulée «Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données» (JO C 124I du 17.4.2020, p. 1).

([7]) Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19 et déclaration du comité européen de la protection des données du 16 juin 2020 sur les conséquences de l'interopérabilité des applications de recherche des contacts sur la protection des données, disponibles à l'adresse: https://edpb.europa.eu/edpb_fr

([8]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

([9]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

([10]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

(10) Les États membres participants, représentés par les autorités nationales ou les organismes officiels désigné(e)s, définissent ensemble la finalité et les moyens du traitement des données à caractère personnel par le biais de la plateforme de fédération et endossent par conséquent le rôle de responsables conjoints du traitement. L'article 26 du règlement général sur la protection des données impose aux responsables conjoints du traitement des données à caractère personnel l'obligation de définir de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences dudit règlement. Cet article prévoit également la possibilité que ces responsabilités soient définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Chaque responsable du traitement devrait s'assurer de disposer d'une base juridique à l'échelle nationale pour le traitement de données sur la plateforme de fédération.

(11) En sa qualité de fournisseur de solutions techniques et organisationnelles pour la plateforme de fédération, la Commission traite des données à caractère personnel pseudonymisées pour le compte des États membres participant à cette plateforme en tant que responsables conjoints du traitement et joue donc le rôle de sous-traitant. Conformément à l'article 28 du règlement général sur la protection des données et à l'article 29 du règlement (UE) 2018/1725, le traitement par un sous-traitant est régi par un contrat ou un acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement et qui définit le traitement. La présente décision définit les règles régissant le traitement des données par la Commission en tant que sous-traitant.

(12) Lorsqu'elle traite des données à caractère personnel dans le cadre de la plateforme de fédération, la Commission est liée par la décision (UE, Euratom) 2017/46 de la Commission ([11]).

(13) Étant donné que les finalités pour lesquelles les responsables du traitement traitent des données à caractère personnel dans le cadre des applications mobiles nationales de suivi de contacts et d'alerte ne nécessitent pas obligatoirement d'identifier les personnes concernées, les responsables du traitement peuvent ne pas être en mesure de garantir systématiquement l'application des droits des personnes concernées. Les droits visés aux articles 15 à 20 du règlement général sur la protection des données peuvent donc ne pas s'appliquer lorsque les conditions fixées à l'article 11 dudit règlement sont remplies.

(14) Il y a lieu de numéroter l'annexe de la décision d'exécution (UE) 2019/1765 en raison de l'ajout de deux nouvelles annexes.

(15) Il convient dès lors de modifier la décision d'exécution (UE) 2019/1765 en conséquence.

(16) Compte tenu de l'urgence de la situation causée par la pandémie de COVID-19, il convient que la présente décision s'applique dès le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

(17) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725, et a rendu son avis le 9 juillet 2020.

(18) Les mesures prévues par la présente décision sont conformes à l'avis du comité institué en vertu de l'article 16 de la directive 2011/24/UE,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

La décision d'exécution (UE) 2019/1765 est modifiée comme suit:

1) À l'article 2, paragraphe 1, les points g), h), i), j), k), l), m), n) et o) suivants sont ajoutés:

«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 (*);

([11]) Décision (UE, Euratom) 2017/46 de la Commission du 10 janvier 2017 sur la sécurité des systèmes d'information et de communication au sein de la Commission européenne (JO L 6 du 11.1.2017, p. 40). La Commission publie des informations complémentaires sur les normes de sécurité applicables à tous les systèmes d'information de la Commission européenne sur la page https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_fr

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;

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.

(*) 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).»

2) À l'article 4, paragraphe 1, le point h) suivant est ajouté:

«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.»

3) À l'article 6, paragraphe 1, les points f) et g) suivants sont ajoutés:

«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.»

4) L'article 7 est modifié comme suit:

a) le titre est remplacé par «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) au paragraphe 2, le terme «annexe» est remplacé par «annexe I».

5) L'article 7 *bis* suivant est inséré:

«*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.

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.»

6) L'annexe devient l'annexe I.

7) Une annexe II et une annexe III, dont le texte figure en annexe de la présente décision, sont ajoutées.

Article 2

La présente décision entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 15 juillet 2020.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

Dans la décision d'exécution (UE) 2019/1765, les annexes II et III suivantes sont ajoutées:

«*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 les «personnes concernées») des informations sur le traitement de leurs données à caractère 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.

([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

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.

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:

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 ([2]);

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:

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.

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.»

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