Traduction

0.818.104.136.1

Accord

entre le Département fédéral de l'intérieur de la Confédération suisse et l'Institut Robert Koch, institut fédéral relevant du ministère fédéral allemand de la Santé, relatif aux applications de traçage du COVID-19 (échange de clés par l'intermédiaire d'un serveur passerelle géré en Suisse afin d'assurer l'interopérabilité transfrontalière)

Conclu le 19 mars 2021
Entré en vigueur par échange de notes le 7 mai 2021
(Etat le 7 mai 2021)

L'Institut Robert Koch, institut fédéral relevant du ministère fédéral allemand de la Santé, en tant que responsable de l'application Corona-Warn-App selon la législation en matière de protection des données, ci-après **«RKI»**, et le Département fédéral de l'intérieur de la Confédération suisse, représenté par l'Office fédéral de la santé publique, en tant que responsable de l'application SwissCovid selon la législation en matière de protection des données, ci-après **«OFSP»**, conjointement désignés **«Partenaires»**, concluent le présent Accord relatif à l'échange de clés de leurs applications de traçage respectives sur un serveur passerelle géré en Suisse, afin de garantir l'interopérabilité transfrontalière.

§ 1 Champ d'application et but de cet accord

1. Le présent Accord se limite au traitement des données à caractère personnel par le serveur passerelle, tel que décrit au § 3, dans le but de permettre le lancement d'alertes transfrontalières entre des utilisateurs de l'application Corona-Warn-App du RKI qui ont été testés positifs au coronavirus et des utilisateurs de l'application SwissCovid de l'OFSP qui ont été testés positifs au coronavirus. Dans la mesure où les Partenaires sont les responsables conjoints de ce traitement selon la législation en matière de protection des données, comme prévu à l'art. 26 du règlement général sur la protection des données (RGPD) ou dans des dispositions nationales équivalentes, les accords suivants s'appliqueront.

2. Le traitement des données par le serveur passerelle a pour seule finalité de permettre au RKI, en tant qu'opérateur de l'application Corona-Warn-App, et à l'OFSP, en tant qu'opérateur de l'application SwissCovid, de disposer de moyens techniques pour avertir efficacement leurs utilisateurs si ces derniers ont été potentiellement exposés au SARS-CoV-2 suite à la présence à proximité d'eux d'un utilisateur de l'autre application nationale de traçage qui a déclenché une alerte. La finalité énoncée ci-dessus comprend aussi la réalisation d'une analyse statistique postérieure des données de journal, afin de s'assurer du bon fonctionnement du serveur passerelle et de pouvoir réaliser un suivi statistique de son exploitation et de son utilisation générale.

3. Le présent Accord a pour but de définir les finalités et les moyens du traitement conjoint et de fixer les droits et obligations des Partenaires à cet égard, en tant que responsables conjoints. Pour les activités de traitement qui ne font pas partie du champ d'application du présent Accord et pour lesquelles aucune finalité ni aucun moyen n'est conjointement défini pour le traitement, chaque Partenaire sera considéré comme un responsable indépendant.

§ 2 Définitions

1. Le terme «utilisateur» désigne une personne qui utilise une application de traçage sur un téléphone mobile.

2. L'expression «applications de traçage» renvoie aux applications logicielles pour téléphone mobile (applications) éditées par les Partenaires sous les appellations «Corona-Warn-App» et «SwissCovid», dans le but d'enregistrer les situations de proximité physique entre les utilisateurs et de les alerter s'ils ont potentiellement été exposés au coronavirus Sars-CoV-2.

3. Un «serveur dorsal» est un système de serveur géré au niveau national, qui met à disposition de l'application nationale (application de traçage ou application correspondante) son contenu dans le cadre d'une procédure d'accès en ligne. Ce contenu comprend notamment les clés et les métadonnées transmises par les «applications de traçage» ou téléchargées depuis le serveur passerelle.

4. Le «serveur passerelle» désigne un système de serveur géré par l'OFSP, auquel un serveur dorsal peut se connecter par le biais d'une interface afin de charger les clés de son application nationale et de télécharger les clés de l'application étrangère correspondante mises à sa disposition.

5. Les «clés» sont des identifiants uniques valables une seule journée, qui sont générés par le système d'exploitation du téléphone mobile (avec les métadonnées associées) pour un utilisateur qui signale sur l'application de traçage de son téléphone qu'il a été testé positif à une infection par le SARS-CoV-2. Ces clés sont considérées comme des données concernant la santé au sens du RGPD.

6. Les «métadonnées» sont des informations reliées à une clé ou incluses dans une clé, qui peuvent contenir des renseignements sur le jour de validité, la vérification de l'infection, le pays d'origine de la clé et d'autres renseignements pertinents du point de vue épidémiologique. Elles sont utilisées par une application de traçage pour évaluer l'infectiosité d'un utilisateur qui déclare avoir été testé positif à une infection par le SARS-CoV-2 par le biais de l'application de traçage de son téléphone.

7. Par «vérification de l'infection», on entend la méthode employée pour confirmer une infection par le SARS-CoV-2, c'est-à-dire sa confirmation par une autorité sanitaire nationale ou par un test en laboratoire.

8. Les «données de journal» désignent l'enregistrement automatique d'un accès en rapport avec le traitement des données par l'intermédiaire du serveur passerelle, qui indique notamment le type de l'activité de traitement effectuée, la date et l'heure de cette activité.

9. Par «données à caractère personnel», on entend toutes les informations qui se rapportent à une personne physique identifiée ou identifiable (ci-après «personne concernée»), dans le cadre du champ d'application du présent Accord.

§ 3 Échange de données transfrontalier entre l'application Corona-Warn-App et l'application SwissCovid par le biais du serveur passerelle

1. L'activité de traitement conjointe des Partenaires sur le serveur passerelle se limite aux étapes suivantes du processus:

a) Authentification des serveurs dorsaux nationaux.

b) Réception des clés par le biais d'une interface de programmation d'application fournie qui permet aux serveurs dorsaux nationaux de charger ces données.

c) Enregistrement sur le serveur passerelle des clés chargées depuis les serveurs dorsaux nationaux.

d) Mise à disposition des clés enregistrées provenant d'Allemagne sur le serveur passerelle en vue d'un téléchargement par le serveur dorsal suisse.

e) Mise à disposition des clés enregistrées provenant de la Confédération suisse sur le serveur passerelle en vue d'un téléchargement par le serveur dorsal allemand.

f) Vérification de la confidentialité et de l'intégrité des clés lors de la réception et de la mise à disposition.

g) Effacement irrémédiable ou destruction des clés enregistrées dès leur téléchargement et leur contrôle par le serveur dorsal destinataire ou 14 jours après leur réception par le serveur dorsal émetteur, selon la première de ces deux échéances.

h) Effacement irrémédiable ou destruction de toutes les données à caractère personnel restantes après l'arrêt de la gestion du serveur passerelle ou l'arrêt unilatéral et définitif de la transmission des clés au serveur passerelle par un Partenaire.

2. Les serveurs dorsaux nationaux ne peuvent transmettre au serveur passerelle que des clés de leur application nationale dont le jour de validité ne remonte pas à plus de 14 jours avant la date de transmission vers le serveur passerelle.

3. La transmission de clés au serveur passerelle ne peut avoir lieu que si l'utilisateur a expressément donné son accord pour le traitement transfrontalier de ses données aux fins du présent Accord.

4. Le traitement sera en principe réalisé sur la base des directives techniques générales d'interopérabilité accessibles au public qui sont applicables dans le réseau eHealth européen, dans la mesure où le présent Accord ne fixe pas d'autres règles et où la législation nationale des Partenaires le permet. Ces directives résultent notam-

ment des spécifications d'interopérabilité pour le rapprochement des chaînes de transmission transfrontalières entre les applications approuvées en date du 16 juin 2020.[1]

5. Le traitement est effectué sous l'acceptation mutuelle des Partenaires et à la condition impérative que le niveau de protection assuré lors du traitement des données à caractère personnel dans le pays du Partenaire soit équivalent à celui du pays d'origine et pour autant qu'une décision d'adéquation de la Commission européenne au sens de l'art. 45 RGPD existe ou que des garanties appropriées au sens de l'art. 46 RGPD soient prévues et que les personnes concernées disposent de droits opposables et de voies de droit effectives.

§ 4 Compétences et obligations de l'OFSP

1. L'OFSP est chargé de mettre en place et de gérer le serveur passerelle. À ce titre, l'OFSP garantira la sécurité et la protection du traitement des données échangées sur le serveur passerelle, y compris leur transmission et leur mise à disposition, et accomplira les tâches définies au par. 3. L'OFSP assume tous les coûts qui en découlent. Chaque Partenaire reste toutefois redevable des coûts d'adaptation à sa propre application.

2. L'efficacité des moyens techniques et organisationnels mis en œuvre pour garantir la sécurité du traitement sur le serveur passerelle sera régulièrement contrôlée, analysée et évaluée par l'OFSP, avec la participation du Centre national pour la cybersécurité (NCSC) et du Préposé fédéral à la protection des données et à la transparence (PFPDT) au moins une fois par semestre et de manière ponctuelle. Le PFPDT est informé par l'OFSP de l'appréciation et de l'évaluation.

3. L'OFSP:

a) met en place et garantit une infrastructure de communication sécurisée, permettant aux serveurs dorsaux des Partenaires d'échanger les données décrites au § 3 al. 2 selon les dispositions du présent Accord;

b) peut, avec l'accord du RKI, mandater un tiers pour gérer le serveur passerelle en qualité de sous-traitant au sens de l'art. 4 ch. 8 RGPD. L'arrangement contractuel avec le sous-traitant devra répondre aux exigences de l'art. 28 RGPD. En cas de désignation d'un sous-traitant pour le traitement des données à caractère personnel des utilisateurs de l'application Corona-Warn-App, l'OFSP veillera à ce que le sous-traitant se soumette à et respecte les obligations de protection de données prévues par le présent Accord. Le sous-traitant ne devrait en principe avoir la possibilité de désigner lui-même un sous-traitant qu'une seule fois. Dans un tel cas, le RKI devra aussi donner son accord. Le RKI est en droit de refuser la désignation d'un sous-traitant ou d'un sous-traitant du sous-traitant pour un juste motif. Sont notamment des justes motifs la désignation d'un sous-traitant par le sous-traitant qui porte atteinte à la situation juridique du RKI selon le présent Accord, le fait que le RKI ait des raisons valables de penser que les obligations contractuelles et/ou légales de protection des données et/ou de sécurité de

[1] Disponibles à l'adresse: https://ec.europa.eu/health/ehealth/key_documents_fr

l'information pourraient ne pas être respectées par le sous-traitant du sous-traitant ou le fait que certains éléments substantiels indiquent que le sous-traitant du sous-traitant agit de façon contraire à la loi, de telle sorte que la confiance en sa fiabilité générale est altérée;

c) s'assure, en cas de connexion d'autres pays au serveur passerelle, que les clés transmises par le serveur dorsal de l'application Corona-Warn-App au serveur passerelle ne sont toujours échangées qu'avec le serveur dorsal de l'application SwissCovid dans le but prévu par le présent Accord, et ne sont en particulier pas transmises aux systèmes d'autres pays;

d) prend toutes les mesures de sécurité organisationnelles, physiques et logiques fondées sur les prescriptions informatiques de l'administration fédérale de la Confédération suisse (Protection informatique de base dans l'administration fédérale)[2] afin de maintenir le fonctionnement du serveur passerelle. Pour cela, l'OFSP:

   aa) désigne un organisme chargé de gérer la sécurité du serveur passerelle, transmettra ses coordonnées au RKI et garantira sa disponibilité pour réagir aux menaces de sécurité,

   bb) assume la responsabilité de la sécurité du serveur passerelle,

   cc) s'assure que toutes les personnes auxquelles un accès au serveur passerelle est accordé sont soumises à des obligations légales, professionnelles ou contractuelles de confidentialité qui sont suffisantes au regard de la qualification des clés en tant que données concernant la santé selon le RGPD ou des dispositions nationales équivalentes et selon le présent Accord;

e) prend toutes les mesures de sécurité nécessaires pour que le bon fonctionnement des serveurs dorsaux des Partenaires ne soit pas perturbé. Pour cela, l'OFSP définit des procédures spécifiques pour la connexion des serveurs dorsaux au serveur passerelle, notamment:

   aa) une procédure d'évaluation des risques, afin de déceler et d'évaluer les menaces potentielles pour le système,

   bb) une procédure d'audit et de vérification:

      i. afin de contrôler la conformité des mesures de sécurité mises en œuvre avec les directives de sécurité applicables pour le traitement (qui, en ce qui concerne les clés, comprend des données concernant la santé), dans le cadre de la protection informatique de base de l'administration fédérale et de la législation suisse en matière de protection des données,

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

2 En particulier les directives Si001 – Protection informatique de base dans l'administration fédérale et Si003 – Sécurité des réseaux dans l'administration fédérale, accessibles sur: www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Directives informatiques > Sécurité.

iii. afin de mener une surveillance visant à identifier les violations de la sécurité et les intrusions non autorisées,

iv. afin d'apporter des modifications pour remédier aux failles de sécurité existantes, et

v. afin de permettre – y compris sur demande du RKI – et de participer à la réalisation d'audits indépendants (y compris des inspections), ainsi qu'à des contrôles des mesures de sécurité (par ex. protection de base selon BSI), et des contrôles de l'autorité de surveillance de la protection des données compétente pour le RKI, de manière à ce que cette autorité puisse accomplir ses tâches légales,

cc) une procédure de contrôle des modifications, afin de documenter et d'estimer les conséquences d'une modification avant sa mise en œuvre et de tenir les responsables informés de toute modification susceptible d'avoir des répercussions sur la communication avec leurs infrastructures et/ou leur sécurité,

dd) la définition d'une procédure de maintenance et de réparation, avec des règles et conditions relatives à la maintenance et/ou la réparation des équipements,

ee) la définition d'une procédure concernant les incidents de sécurité (programme de signalement et d'escalade), afin de veiller à ce que le délégué à la protection des données du RKI soit immédiatement averti de toute violation de la protection des données à caractère personnel avec indication du type, de l'ampleur et des circonstances de cette violation et de ses conséquences potentielles, ainsi que des mesures prises et prévues pour remédier à cette violation et atténuer ses éventuelles conséquences préjudiciables,

ff) la définition d'une procédure disciplinaire, si une telle procédure n'existe pas déjà, afin d'agir contre les violations de la sécurité,

gg) un test d'intrusion réalisé par un organisme indépendant, avec une analyse du code source;

f) prend des mesures de sécurité physiques et/ou logiques fondées sur l'état actuel de la technique pour les installations dans lesquelles l'équipement du serveur passerelle se trouve et pour les contrôles des données logiques et de la sécurité d'accès. La protection informatique de base (voir § 4 al. 3 let. e bb) i.) servira de référence. Les autres mesures de sécurité techniques et opérationnelles devront être documentées dans le concept de sécurité;

g) prend des mesures pour protéger ses domaines réseau, y compris une séparation des connexions;

h) applique un plan de gestion des risques en ce qui concerne le serveur passerelle;

i) surveille – en temps réel – le fonctionnement de tous les composantes de service du serveur passerelle, établira des statistiques régulières et tiendra des registres au sujet des activités du serveur passerelle;

j) propose un support pour tous les services du serveur passerelle, par téléphone ou par e-mail, et réponds aux les appels des appelants autorisés;

k) prend toutes les mesures nécessaires pour que l'opérateur technique du serveur passerelle ne dispose pas d'un accès non autorisé aux données transmises;

l) prend des mesures pour faciliter la communication entre les Partenaires;

m) tient un registre de toutes les procédures de traitement réalisées selon l'art. 30 al. 1 du RGPD ou selon des dispositions nationales équivalentes et dans le cadre du présent Accord;

n) prend des mesures afin de s'assurer à intervalles réguliers que les mesures de sécurité physiques et logiques restent conformes à l'état actuel de la technique;

o) après concertation avec l'Office fédéral de l'informatique et de la télécommunication (OFIT), permet au RKI ou à des parties prenantes du RKI, telles que l'Office allemand de la sécurité dans les technologies de l'information (BSI), de mener leurs propres analyses techniques de la sécurité du serveur passerelle et de les réitérer en partie ou en totalité si des modifications physiques ou logiques sont apportées au serveur passerelle.

4. L'OFSP communique sans délai au RKI tous les faits et changements importants qui concernent le serveur passerelle et qui ont des répercussions sur le traitement des données échangées sur le serveur passerelle, notamment:

a) les risques potentiels ou effectifs pour la disponibilité, la confidentialité et/ou l'intégrité des données traitées sur le serveur passerelle;

b) les incidents de sécurité;

c) toute violation de la protection des données à caractère personnel, les conséquences probables d'une telle violation de la protection des données à caractère personnel et une évaluation des risques pour les droits et libertés des personnes physiques, ainsi que toutes les mesures qui ont été prises pour agir contre la violation de la protection des données à caractère personnel et pour limiter le risque pour les droits et libertés des personnes physiques;

d) tout manquement aux dispositions techniques et/ou organisationnelles prises dans le cadre du présent Accord pour les procédures de traitement sur le serveur passerelle;

e) toute modification physique ou logique du serveur passerelle ayant une influence directe ou indirecte sur la disponibilité, la confidentialité et/ou l'intégrité des données traitées sur le serveur passerelle.

5. Si un incident de sécurité se produit, l'OFSP doit aussi en informer directement et sans délai le délégué à la protection des données du RKI, afin de convenir des suites à donner. Dans la mesure où, à la suite d'un incident de sécurité, les Partenaires doivent remplir certaines obligations de notification et de communication en vertu des art. 33 et 34 RGPD, l'OFSP mettra immédiatement à la disposition du RKI, et de

façon distincte au délégué à la protection des données du RKI, toutes les informations nécessaires pour vérifier l'existence éventuelle d'une telle obligation de notification ou de communication.

6. Si les Partenaires sont soumis à des obligations de communication en vertu de l'art. 34 RGPD, l'OFSP se charge de communiquer avec les personnes concernées par la violation de la protection des données à caractère personnel en Suisse, y compris les utilisateurs de l'application SwissCovid.

7. L'OFSP est responsable du traitement et de répondre aux éventuelles questions / demandes d'un utilisateur de l'application SwissCovid au sujet de l'exercice des droits des personnes concernées conformément au RGPD ou aux dispositions nationales équivalentes et au présent Accord.

8. Dans le cadre de la déclaration de protection des données de l'application SwissCovid, l'OFSP informera les utilisateurs de l'application SwissCovid conformément aux art. 13 et 14 et à l'art. 26 al. 2 ch. 2 RGPD du traitement de leurs données à caractère personnel réalisé selon le présent Accord dans le but de permettre des alertes transfrontalières.

§ 5 Compétences et obligations du RKI

1. Dans la mesure du possible, le RKI soutient l'OFSP lors de l'évaluation et du traitement des incidents de sécurité (y compris les violations de la protection des données à caractère personnel) en rapport avec le traitement réalisé sur le serveur passerelle.

2. Dans la mesure où il en est informé et où il le peut, le RKI signale notamment à l'OFSP:

a) les risques potentiels ou effectifs pour la disponibilité, la confidentialité et/ou l'intégrité des données à caractère personnel traitées sur le serveur passerelle;

b) les incidents de sécurité en rapport avec le traitement réalisé sur le serveur passerelle;

c) toute violation de la protection des données à caractère personnel, les conséquences probables d'une telle violation de la protection des données à caractère personnel et une évaluation des risques pour les droits et libertés des personnes physiques, ainsi que toutes les mesures qui ont été prises pour agir contre la violation de la protection des données à caractère personnel et pour limiter le risque pour les droits et libertés des personnes physiques;

d) tout manquement aux dispositions techniques et/ou organisationnelles prises pour les procédures de traitement sur le serveur passerelle.

3. Le RKI est responsable du traitement et de répondre aux éventuelles questions / demandes d'un utilisateur de l'application Corona-Warn-App au sujet de l'exercice des droits des personnes concernées conformément au RGPD ou aux dispositions nationales équivalentes et au présent Accord.

4. Dans le cadre de la déclaration de protection des données de l'application Corona-Warn-App, le RKI informe les utilisateurs de l'application Corona-Warn-App,

comme prévu aux art. 13 et 14 et à l'art. 26 al. 2 ch. 2 du RGPD du traitement de leurs données à caractère personnel réalisé selon le présent Accord.

5. Les obligations de notification ou de communication qui incombent aux Partenaires selon les art. 33 et 34 RGPD sont sous la responsabilité du RKI. Le RKI st responsable de la mise en œuvre des notifications et des communications ainsi que de la communication avec l'autorité de surveillance compétente au sens des art. 33 et 34 RGPD.

6. Si les Partenaires sont soumis à des obligations de communication selon l'art. 34 RGPD, le RKI se charge de communiquer avec les personnes concernées par la violation de la protection des données à caractère personnel en Allemagne, y compris les utilisateurs de l'application Corona-Warn-App.

§ 6 Compétences et obligations des deux Partenaires

1. Chaque Partenaire met en place un point de contact avec une boîte aux lettres fonctionnelle qui servira à la communication entre les Partenaires dans le cadre du présent Accord. Par principe, les courriers reçus doivent être consultés dans un délai très bref et il convient d'y répondre rapidement. En cas d'urgence, il faut également prendre contact avec l'autre Partenaire par téléphone, pour information et concertation. Chaque Partenaire désigne dans ce but un interlocuteur direct (e-mail, téléphone).

2. Chaque Partenaire traite les questions / demandes qui lui sont transmises par les utilisateurs au sujet de l'exercice des droits des personnes concernées, en accord avec le RGPD ou des dispositions nationales équivalentes et avec le présent Accord. Chaque Partenaire désigne un point de contact spécifique pour les questions / demandes des utilisateurs. Si un Partenaire reçoit une question / demande d'un utilisateur au sujet de l'exercice des droits des personnes concernées qui ne relève pas de sa compétence ou de sa responsabilité selon le présent Accord ou les dispositions juridiques auxquelles il est soumis, il devra la transférer sans délai au Partenaire compétent. Les Partenaires s'assistent mutuellement en vue du traitement des questions / demandes des personnes concernées au sujet de l'exercice des droits des personnes concernées sur simple demande et se transmettront des réponses au plus vite, dans tous les cas sous 15 jours après réception d'une demande d'assistance.

3. Chaque Partenaire publie le présent Accord sur son site Internet.

4. Si un Partenaire a besoin d'obtenir auprès de l'autre Partenaire des informations afin de remplir ses obligations selon les art. 35 et 36 RGPD ou des dispositions nationales équivalentes et selon le présent Accord, il doit envoyer une demande spéciale à la boîte aux lettres fonctionnelle de l'autre Partenaire. Ce dernier fait tout son possible pour fournir ces informations.

5. Chaque Partenaire est tenu de veiller à l'exactitude des données à caractère personnel qui doivent être transmises sur le serveur passerelle. S'il s'avère qu'un Partenaire a transmis sur le serveur passerelle des données à caractère personnel

inexactes ou des données à caractère personnel qui n'auraient pas dû être transmises, il devra en informer immédiatement l'autre Partenaire.

6. Les données à caractère personnel des utilisateurs d'une application de traçage qui sont transmises par les Partenaires sur le serveur passerelle ne peuvent l'être que sous une forme anonymisée ou pseudonymisée. Chacun des Partenaires atteste qu'il ne lui est pas possible, dans l'état actuel des connaissances:

a) de tirer des conclusions sur l'identité des utilisateurs concrets à l'aide des clés présentes sur son serveur dorsal, et

b) de tirer des conclusions sur l'identité des utilisateurs concrets à l'aide des clés qu'il a reçues de l'autre Partenaire via le serveur passerelle, et à l'aide d'autres données éventuelles.

7. Si un Partenaire ne peut pas traiter les questions / demandes d'une personne concernée au sujet de l'exercice des droits des personnes concernées parce qu'il ne peut pas l'identifier suite à sa désactivation délibérée de la fonction de traçage, il devra en informer la personne concernée si les données de contact dont il dispose (par ex. adresse e-mail, adresse postale) le lui permettent. Dans ce cas, les droits des personnes concernées ne s'appliqueront pas, sauf si la personne concernée met à disposition des informations supplémentaires permettant de l'identifier en vue de l'exercice de ses droits légaux.

8. Chaque Partenaire s'assure que l'autre Partenaire ou l'entité juridique qui la représente selon le droit national applicable assume sa responsabilité envers la personne qui a subi un dommage illicite suite à la transmission de données dans le cadre du présent Accord. Les dispositions de l'art. 82 al. 4 et al. 5 RGPD ou des dispositions nationales équivalentes prévoyant qu'il existe une responsabilité solidaire des responsables conjoints envers les tiers s'appliquent aux relations entre les Partenaires, avec toutefois une répartition en fonction de la part de responsabilité de l'événement préjudiciable.

§ 7 Règlement des litiges

1. En cas de litige entre les Partenaires au sujet de l'interprétation ou de l'application du présent Accord, les Partenaires s'efforceront de le régler à l'amiable, dans la mesure du possible.

2. S'il est impossible de régler un litige de cette manière, un Partenaire pourra le soumettre à un tribunal arbitral.

3. Ce tribunal d'arbitrage sera constitué au cas par cas, chaque Partenaire désignant un membre et les deux membres s'associant à un troisième membre agissant en tant que président ou présidente, désigné(e) par les deux Partenaires. Les membres seront nommés dans un délai de deux semaines à compter de la date à laquelle un Partenaire informe l'autre qu'il souhaite soumettre le litige à un tribunal arbitral.

4. Le tribunal arbitral prendra ses décisions à la majorité des voix. Ses décisions auront force obligatoire et seront sans appel. Chaque Partenaire assumera les frais engagés par le membre qu'il a désigné et les frais nécessaires pour sa suppléance lors de la procédure auprès du tribunal d'arbitrage; les frais du président ou de la

présidente ainsi que les autres frais seront assumés à parts égales par les Partenaires. Le tribunal arbitral pourra prendre d'autres dispositions concernant les frais. Au demeurant, le tribunal arbitral fixera sa propre procédure.

§ 8 Dispositions finales

1. Le présent Accord entrera en vigueur dès que les Partenaires se seront mutuellement informés que les conditions requises au niveau national sont remplies. Le serveur passerelle entrera en fonction dès que l'ensemble des installations requises seront prêtes.

2. Le présent Accord peut être modifié, résilié ou prolongé à tout moment, d'un commun accord entre les Partenaires.

3. Le présent Accord restera en vigueur pendant toute la durée des échanges de clés entre les deux Partenaires via le serveur passerelle et aussi longtemps que le serveur passerelle existera, une date butoir étant toutefois fixée au 30 juin 2022.

4. Les dispositions du présent Accord relatives à la protection des données à caractère personnel resteront applicables aux données déjà transmises même en cas de résiliation, de dénonciation ou d'expiration de cet accord.

5. Chaque Partenaire peut à tout moment cesser de transmettre au serveur passerelle des clés concernant les utilisateurs de son application de traçage. Dans la mesure du possible, une telle décision doit être communiquée au plus tôt à l'autre Partenaire, afin que celui-ci puisse rapidement prendre les mesures nécessaires, comme une modification des informations relatives à la protection des données pour les utilisateurs de son application de traçage.

6. Le présent Accord peut être résilié de façon unilatérale par chacun des Partenaires, moyennant l'envoi d'une notification écrite. La résiliation sera effective à l'expiration d'un délai d'un mois après réception de la notification par l'autre Partenaire.

Berne, le 15 mars 2021

Pour
le Département fédéral de l'intérieur:

Anne Lévy

Berlin, le 19 mars 2021

Pour
l'Institut Robert Koch:

Lars Schaade