

FEDERALE OVERHEIDSDIENST
KANSELARIJ
VAN DE EERSTE MINISTER

[C – 2020/10440]

13 OKTOBER 2020. — Uitvoerend samenwerkingsakkoord tussen de Federale Staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie, betreffende de digitale contactopsporingsapplicatie(s), overeenkomstig artikel 92bis, §1, derde lid, van de Bijzondere wet van 8 augustus 1980 tot hervorming der instellingen

Gelet op de Bijzondere wet van 8 augustus 1980 tot hervorming der instellingen, artikel 92bis, § 1, derde lid, ingevoegd bij de Bijzondere wet van 6 januari 2014;

Gelet op het samenwerkingsakkoord van 25 augustus 2020 tussen de Federale Staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie, betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde gefedereerde entiteiten of door de bevoegde agentenschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano, artikel 14, § 9;

Gelet op het advies nr. 79/2020 van de Gegevensbeschermingsautoriteit, gegeven op 7 september 2020;

Gelet op het advies nr. 2020/37 van de Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens, gegeven op 14 september 2020;

Gelet op de kennisgeving nr. 2020/0546/B aan de Europese Commissie met toepassing van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 bij de Europese Commissie;

Overwegende dat krachtens het artikel 92bis, § 1, derde lid, van de Bijzondere wet van 8 augustus 1980 tot hervorming der instellingen, het samenwerkingsakkoord, dat de instemming heeft gekregen van de betrokken parlementen, kan voorzien dat de uitvoering ervan zal worden verzekerd door uitvoerende samenwerkingsakkoorden die gelden zonder dat de instemming bij wet of decreet vereist is;

Overwegende dat de partijen streven naar een effectieve werking van de digitale contactopsporingsapplicatie(s) op een wijze die het minst invasief is op het vlak van de het recht op bescherming van de persoonlijke levenssfeer;

De Belgische Staat, vertegenwoordigd door zijn regering in de persoon van Alexander De Croo, Eerste Minister, en Frank Vandembroucke, Vice-Eerste Minister en Minister van Sociale Zaken en Volksgezondheid;

De Vlaamse Gemeenschap, vertegenwoordigd door zijn regering in de persoon van Jan Jambon, Minister-President van de Vlaamse Regering en Vlaams Minister van Buitenlandse Zaken, Cultuur, ICT en Facilitair Management, en Wouter Beke, Vlaams Minister van Welzijn, Volksgezondheid, Gezin en Armoedebestrijding;

SERVICE PUBLIC FEDERAL
CHANCELLERIE
DU PREMIER MINISTRE

[C – 2020/10440]

13 OCTOBRE 2020. — Accord de coopération d'exécution entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant la ou les applications numériques de traçage des contacts, conformément à l'article 92bis, § 1^{er}, alinéa 3, de la loi spéciale de réformes institutionnelles du 8 août 1980

Vu la loi spéciale de réformes institutionnelles du 8 août 1980, article 92bis, § 1^{er}, alinéa 3, inséré par la loi spéciale du 6 janvier 2014;

Vu l'accord de coopération du 25 août 2020 conclu entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présomées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano, article 14, § 9;

Vu l'avis n° 79/2020 de l'Autorité de protection des données, donné le 7 septembre 2020;

Vu l'avis n° 2020/37 du "Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens" donné le 14 septembre 2020;

Vu la notification n° 2020/0546/B à la Commission européenne en application de la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 ;

Considérant qu'en vertu de l'article 92bis, § 1^{er}, alinéa 3, de la loi spéciale de réformes institutionnelles du 8 août 1980, l'accord de coopération, qui a reçu l'assentiment des parlements concernés, peut prévoir que sa mise en œuvre sera assurée par des accords de coopération d'exécution ayant effet sans que l'assentiment par la loi ou le décret ne soit requis;

Considérant que les parties aspirent à un fonctionnement effectif de la ou des applications numériques de traçage des contacts d'une manière qui soit la moins invasive possible sur le plan du droit à la protection de la vie privée;

L'Etat belge, représenté par son gouvernement en la personne d'Alexander De Croo, Premier Ministre, et de Frank Vandembroucke, Vice-Premier Ministre et Ministre des Affaires sociales et de la Santé publique ;

La Communauté flamande, représentée par son gouvernement en la personne de Jan Jambon, Ministre-Président du Gouvernement flamand et Ministre flamand de la Politique extérieure, de la Culture, la TI et les Services généraux, et de Wouter Beke, Ministre flamand du Bien-Être, de la Santé publique, de la Famille et de la Lutte contre la Pauvreté ;

FÖDERALER ÖFFENTLICHER DIENST
KANZLEI
DES PREMIERMINISTERS

[C – 2020/10440]

13 OKTOBER 2020 — Ausführendes Zusammenarbeitsabkommen zwischen dem Föderalstaat, der Flämischen Gemeinschaft, der Wallonischen Region, der Deutschsprachigen Gemeinschaft und der Gemeinsamen Gemeinschaftskommission in Bezug auf die digitale(n) Kontakttrückverfolgungsanwendung(en), abgeschlossen gemäß Artikel 92bis § 1 Absatz 3 des Sondergesetzes vom 8. August 1980 zur Reform der Institutionen

Aufgrund des Sondergesetzes vom 8. August 1980 zur Reform der Institutionen, des Artikels 92bis § 1 Absatz 3, eingefügt durch das Sondergesetz vom 6. Januar 2014;

Aufgrund des Zusammenarbeitsabkommens vom 25. August 2020 zwischen dem Föderalstaat, der Flämischen Gemeinschaft, der Wallonischen Region, der Deutschsprachigen Gemeinschaft und der Gemeinsamen Gemeinschaftskommission in Bezug auf die gemeinsame Verarbeitung von Daten durch Sciensano und die von den zuständigen föderierten Teilgebieten oder von den zuständigen Agenturen bestimmten Kontaktzentren, Gesundheitsinspektionsdiensten und mobilen Teams im Rahmen einer Kontaktermittlung bei (vermutlich) mit dem Coronavirus COVID-19 infizierten Personen auf der Grundlage einer Datenbank bei Sciensano, des Artikels 14 § 9;

Aufgrund des Gutachtens Nr. 79/2020 der Datenschutzbehörde erteilt am 7. September 2020;

Aufgrund des Gutachtens Nr. 2020/37 der „Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens“ erteilt am 14. September 2020;

Aufgrund der Notifizierung Nr. 2020/0546/B an die Europäische Kommission in Anwendung der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015;

In der Erwägung, dass aufgrund des Artikels 92bis § 1 Absatz 3 des Sondergesetzes vom 8. August 1980 zur Reform der Institutionen Zusammenarbeitsabkommen, die von den betreffenden Parlamenten gebilligt worden sind, vorsehen können, dass ihre Ausführung durch ausführende Zusammenarbeitsabkommen sichergestellt wird, die wirksam sind, ohne dass sie durch Gesetz oder Dekret gebilligt werden müssen;

In der Erwägung, dass die Vertragsparteien eine wirksame Funktionsweise der digitale(n) Kontakttrückverfolgungsanwendung(en) anstreben, die hinsichtlich des Rechts auf Schutz des Privatlebens möglichst wenig invasiv ist;

Der Belgische Staat, vertreten durch seine Regierung in der Person von Alexander De Croo, Premierminister, und von Frank Vandembroucke, Minister der Sozialen Angelegenheiten und der Volksgezundheit, mit Sitz in 1000 Brüssel;

Die Flämische Gemeinschaft, vertreten durch ihre Regierung in der Person von Jan Jambon, Ministerpräsident der Flämischen Regierung und Flämischer Minister der Außenpolitik, der Kultur, der IKT und der Allgemeinen Dienste, und von Wouter Beke, Flämischer Minister des Wohlbefindens, der Volksgezundheit, der Familie und der Armutsbekämpfung;

Het Waalse Gewest, vertegenwoordigd door zijn regering in de persoon van Elio Di Rupo, Minister-President van de Waalse Regering, Christie Morreale, Vice-Minister-President van de Waalse Regering en Minister van Werk, Vorming, Gezondheid, Sociale Actie, Gelijke Kansen en Vrouwenrechten en Willy BORSUS, Vice-Minister-President van Wallonië en Minister van Economie, Buitenlandse Handel, Onderzoek en Innovatie, Digitale technologieën, Landbouw, Ruimtelijke Ordening, het "IFAPME" en de Vaardigheidscentra ;

De Duitstalige Gemeenschap, vertegenwoordigd door zijn regering in de persoon van Oliver Paasch, Minister-President en Minister van Lokale Besturen en Financiën en Antonios Antoniadis, Vice-Minister-President en Minister van Gezondheid en Sociale Aangelegenheden, Ruimtelijke Ordening en Huisvesting ;

De Gemeenschappelijke Gemeenschapscommissie, vertegenwoordigd door het Verenigd College in de persoon van Rudi Vervoort, Voorzitter van het Verenigd College en Alain Maron en Elke Van Den Brandt, leden belast met Gezondheid en Welzijn ;

Hierna de contracterende partijen genoemd,

Gezamenlijk hun eigen bevoegdheden uitoefenend, komen overeen wat volgt:

HOOFDSTUK I. — *Définitions*

Artikel 1. Voor de toepassing van dit akkoord wordt verstaan onder:

1° samenwerkingsakkoord: het samenwerkingsakkoord van 25 augustus 2020 tussen de Federale Staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie, betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde overheden of door de agentschappen van de gefedereerde entiteiten aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano;

2° Gegevensbank I: de Gegevensbank I bedoeld in artikel 1, § 1, 6° van het samenwerkingsakkoord;

3° Gegevensbank V: de Gegevensbank V bedoeld in artikel 1, § 1, 10° van het samenwerkingsakkoord;

4° Gegevensbank VI: een gegevensbank waarvoor Sciensano de verwerkingsverantwoordelijke is en waarin zeer tijdelijk de testresultaten worden opgeslagen, samen met de testcode, de datum van staalafname en de datum waarop de gebruiker besmettelijk is geworden overeenkomstig het proces beschreven in artikel 2, § 1, 3°;

5° test: een coronavirus COVID-19 test waarmee wordt nagegaan of een persoon met het coronavirus COVID-19 besmet is;

6° app: de digitale contactopsporingsapplicatie CoronAlert, die door de gefedereerde entiteiten ter beschikking wordt gesteld;

7° beveiligde sleutel: een beveiligde sleutel die na installatie van de app elke dag wordt gegenereerd en opgeslagen op de smartphone waarop de app is geïnstalleerd;

La Région wallonne, représentée par son gouvernement en la personne de Elio Di Rupo, Ministre-Président du Gouvernement wallon, Christie Morreale, Vice-Présidente du Gouvernement wallon et Ministre de l'Emploi, de la Formation, de la Santé, de l'Action sociale, de l'Égalité des chances et des Droits des femmes, et de Willy BORSUS, Vice-Président de la Wallonie et Ministre de l'Économie, du Commerce extérieur, de la Recherche et de l'Innovation, du Numérique, de l'Agriculture, de l'Aménagement du territoire, de l'IFAPME et des Centres de compétence ;

La Communauté germanophone, représentée par son gouvernement en la personne de Oliver Paasch, Ministre-Président et Ministre des Pouvoirs locaux et des Finances et Antonios Antoniadis, Vice-Ministre-Président et Ministre de la Santé et des Affaires sociales, de l'Aménagement du territoire et du Logement ;

La Commission communautaire commune, représentée par le Collège réuni en la personne de Rudi Vervoort, Président du Collège réuni et Alain Maron et Elke Van den Brandt, membres ayant la Santé et l'Action sociale dans leurs attributions ;

Ci-après appelés les parties contractantes,

Exerçant conjointement leurs compétences propres, conviennent de ce qui suit:

CHAPITRE I^{er}. — *Définitions*

Article 1^{er}. Aux fins du présent accord, on entend par :

1° accord de coopération: l'accord de coopération du 25 août 2020 entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités compétentes ou par les agences des entités fédérées, par les services d'inspection d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présymptées) infectées par le coronavirus COVID-19 se fondant sur une base de données auprès de Sciensano;

2° Base de données I : la Base de données I visée à l'article 1, § 1, 6° de l'accord de coopération;

3° Base de données V : la Base de données V visée à l'article 1, § 1, 10° de l'accord de coopération;

4° Base de données VI: une base de données pour laquelle Sciensano est le responsable du traitement et dans laquelle sont enregistrés, de manière très temporaire, les résultats du test ainsi que le code du test, la date du prélèvement et la date à laquelle l'utilisateur est devenu contagieux, conformément au processus décrit à l'article 2, § 1^{er}, 3°;

5° test: un test de dépistage du coronavirus COVID-19 permettant de constater qu'une personne est infectée par le coronavirus COVID-19;

6° appli: l'application numérique de traçage des contacts CoronAlert, qui est mise à la disposition par les entités fédérées;

7° clé sécurisée : une clé sécurisée qui, après installation de l'appli, est générée quotidiennement et enregistrée sur le smartphone sur lequel l'appli est installée;

Die Wallonische Region, vertreten durch ihre Regierung in der Person von Elio Di Rupo, Ministerpräsident der Wallonischen Regierung, von Christie Morreale, Vizepräsidentin der Wallonischen Regierung und Ministerin für Beschäftigung, Ausbildung, Gesundheit, Soziale Maßnahmen, Chancengleichheit und Frauenrechte, und von Willy Borsus, Vizepräsident der Wallonie und Minister für Wirtschaft, Außenhandel, Forschung und Innovation, Digitale Technologien, Landwirtschaft, Raumordnung, das IFAPME und die Kompetenzzentren;

Die Deutschsprachige Gemeinschaft, vertreten durch ihre Regierung in der Person von Oliver Paasch, Ministerpräsident und Minister für lokale Behörden und Finanzen, und von Antonios Antoniadis, Vize-Ministerpräsident und Minister für Gesundheit und Soziales, Raumordnung und Wohnungswesen;

Die Gemeinsame Gemeinschaftskommission, vertreten durch das Vereinigte Kollegium in der Person von Rudi Vervoort, Präsident des Vereinigten Kollegiums, und von Alain Maron und Elke Van den Brandt, für die Gesundheit und die Soziale Aktion zuständige Mitglieder;

Nachfolgend "Vertragsparteien" genannt,

Zusammen ihre eigenen Befugnisse ausübend, vereinbaren Folgendes:

KAPITEL I - Begriffsbestimmungen

Artikel 1 - Für die Anwendung des vorliegenden Abkommens versteht man unter:

1° Zusammenarbeitsabkommen: das Zusammenarbeitsabkommen vom 25. August 2020 zwischen dem Föderalstaat, der Flämischen Gemeinschaft, der Wallonischen Region, der Deutschsprachigen Gemeinschaft und der Gemeinsamen Gemeinschaftskommission in Bezug auf die gemeinsame Verarbeitung von Daten durch Sciensano und die von den zuständigen föderierten Teilgebieten oder von den zuständigen Agenturen bestimmten Kontaktzentren, Gesundheitsinspektionsdiensten und mobilen Teams im Rahmen einer Kontakt-ermittlung bei (vermutlich) mit dem Coronavirus COVID-19 infizierten Personen auf der Grundlage einer Datenbank bei Sciensano,

2° Datenbank I: die in Artikel 1 § 1 Nr. 6 des Zusammenarbeitsabkommens erwähnte Datenbank I,

3° Datenbank V: die in Artikel 1 § 1 Nr. 10 des Zusammenarbeitsabkommens erwähnte Datenbank V,

4° Datenbank VI: Datenbank, für die Sciensano der für die Verarbeitung Verantwortliche ist und in der für einen sehr begrenzten Zeitraum Testergebnisse, Testcode, Datum der Probenentnahme und Datum, an dem der Benutzer ansteckend geworden ist, gespeichert werden gemäß dem in Artikel 2 § 1 Nr. 3 erwähnten Protokoll,

5° Test: COVID-19-Coronavirustest, mit dem überprüft wird, ob eine Person mit dem Coronavirus COVID-19 infiziert ist,

6° App: die digitale Kontaktrückverfolgungsanwendung CoronAlert, die von den föderierten Teilgebieten zur Verfügung gestellt wird,

7° Sicherheitsschlüssel: Sicherheitsschlüssel, der nach Installierung der App täglich generiert und auf dem Smartphone gespeichert wird, auf dem die App installiert ist,

8° niet-gepersonaliseerd tijdelijk serienummer: willekeurige combinatie van enen en nullen, die door een smartphone waarop de app is geïnstalleerd via een Bluetooth baken wordt uitgezonden en die bestaat uit een willekeurig getal en de vercijfering van anonieme gegevens van de smartphone, zoals de sterkte van het verzonden signaal;

9° autorisatiecode: de anonieme autorisatiecode die de Gegevensbank VI aanmaakt om de gebruiker die positief getest is toe te laten beveiligde sleutels op te laden in Gegevensbank V;

10° risicocontact: een contact gedurende minstens vijftien minuten binnen een afstand van minder dan twee meter met een besmet persoon; dat contact wordt vastgesteld wanneer op een smartphone een niet-gepersonaliseerd tijdelijk serienummer wordt gevonden dat overeenkomt met een niet-gepersonaliseerd serienummer dat werd uitgezonden door de smartphone van een besmette gebruiker;

11° testnummer: willekeurige combinatie van enen en nullen, die wordt gebruikt om aan te tonen dat de beveiligde sleutels afkomstig zijn van een correcte app, met name een authentieke Coronalert app die geïnstalleerd is op de smartphone van de gebruiker op het moment dat hij/zij een test aanvraagt, zonder deze app te identificeren;

12° testcode: een code die bestaat uit willekeurige cijfers en wordt aangemaakt door de app bij de aanvraag van een test.

HOOFDSTUK II. — *Algemeen*

Art. 2. § 1. Overeenkomstig artikel 14, § 1 van het samenwerkingsakkoord biedt de app de volgende functionaliteiten aan en voert volgende verwerkingen uit:

1° Het registreren, op niet-gepersonaliseerde wijze, van de contacten van de gebruiker van de app met andere gebruikers van de app:

a) elke app genereert elke dag een andere beveiligde sleutel;

b) de beveiligde sleutel is enkel gekend op de smartphone waarop de app is geïnstalleerd;

c) op basis van de beveiligde sleutel worden niet-gepersonaliseerde tijdelijke serienummers gegenereerd;

d) op regelgebaseerde wijze stuurt elke smartphone waarop de app is geïnstalleerd een niet-gepersonaliseerde tijdelijk serienummer uit als een Bluetooth baken; minstens om de twintig minuten wordt een ander niet-gepersonaliseerd tijdelijk serienummer uitgezonden om te beletten dat deze niet-gepersonaliseerde tijdelijke serienummers kunnen gebruikt worden om een gebruiker te volgen; na de uitzendperiode wordt een niet-gepersonaliseerd tijdelijk serienummer niet bewaard op de smartphone die het serienummer verzonden heeft;

e) elke smartphone waarop de app is geïnstalleerd, slaat de Bluetooth bakens met de niet-gepersonaliseerde tijdelijke serienummers op die door andere smartphones op een beperkte afstand worden uitgezonden, samen met de dag waarop het baken is ontvangen en de signaalsterkte;

f) de niet-gepersonaliseerde tijdelijke serienummers worden bewaard op de ontvangende smartphone gedurende veertien dagen en daarna verwijderd.

2° Het aanmaken en overmaken van een testcode bij de aanvraag van een test:

8° numéro de série temporaire non personnalisé: combinaison aléatoire de uns et de zéros, émise par un smartphone sur lequel l'appli est installée au moyen d'une balise Bluetooth qui se compose d'un chiffre aléatoire et du chiffrement de données anonymes du smartphone, comme la puissance du signal émis;

9° code d'autorisation: le code d'autorisation anonyme créé par la Base de données VI afin de permettre à l'utilisateur dont le test s'est révélé positif à charger les clés sécurisées dans la Base de données V;

10° contact à risque: un contact pendant au moins quinze minutes à moins de deux mètres de distance avec une personne infectée; ce contact est établi lorsqu'un numéro de série temporaire non personnalisé correspondant à un numéro de série non personnalisé émis par le smartphone d'un utilisateur infecté est trouvé sur un smartphone;

11° numéro de test: combinaison aléatoire de uns et de zéros, utilisée pour prouver que les clés sécurisées proviennent d'une appli correcte, à savoir d'une appli authentique Coronalert qui est installée sur le smartphone de l'utilisateur au moment où il demande un test, sans que cette appli ne soit identifiée;

12° code de test: un code qui se compose de chiffres aléatoires et qui est créé par l'appli lors de la demande d'un test.

CHAPITRE II. — *Généralités*

Art. 2. § 1^{er}. Conformément à l'article 14, § 1^{er}, de l'accord de coopération, l'appli offre les fonctionnalités suivantes et réalise les opérations suivantes:

1° L'enregistrement, de façon non-personnalisée, des contacts de l'utilisateur de l'appli avec d'autres utilisateurs de l'appli:

a) chaque appli génère chaque jour une nouvelle clé sécurisée;

b) la clé sécurisée est uniquement connue sur le smartphone sur lequel l'appli est installée;

c) sur la base de la clé sécurisée sont générés des numéros de série temporaires non personnalisés;

d) à une fréquence régulière, tout smartphone sur lequel l'appli est installée émet un numéro de série temporaire non personnalisé en tant que balise Bluetooth; un autre numéro de série temporaire non personnalisé est envoyé, au moins toutes les vingt minutes, afin d'empêcher que ces numéros de série temporaires non personnalisés soient utilisés pour suivre un utilisateur; après la période d'émission, un numéro de série temporaire non personnalisé n'est pas enregistré sur le smartphone qui a envoyé le numéro de série;

e) chaque smartphone sur lequel l'appli est installée, enregistre les balises Bluetooth contenant les numéros de série temporaires non personnalisés qui sont émises par d'autres smartphones se trouvant à une distance réduite, ainsi que le jour de réception de la balise et la puissance du signal;

f) les numéros de série temporaires non personnalisés sont conservés sur le smartphone qui les reçoit pendant quatorze jours et sont ensuite supprimés.

2° La création et la transmission d'un code de test lors de la demande d'un test:

8° nicht personalisierter zeitweiliger Seriennummer: zufällige Kombination von Einsen und Nullen, die von einem Smartphone, auf dem die App installiert ist, mittels einer Bluetooth-Bake ausgesendet wird und aus einer Zufallszahl und der Verschlüsselung anonymer Daten des Smartphones besteht, so die Stärke des ausgesendeten Signals,

9° Ermächtigungscode: durch die Datenbank VI erstellter anonymer Ermächtigungscode, mit dem dem Benutzer, dessen Test positiv ist, ermöglicht wird, die Sicherheitsschlüssel in die Datenbank V hochzuladen,

10° Risikokontakt: Kontakt während mindestens fünfzehn Minuten in einer Entfernung von weniger als zwei Metern mit einer infizierten Person; dieser Kontakt wird festgestellt, wenn auf einem Smartphone eine nicht personalisierte zeitweilige Seriennummer gefunden wird, die einer nicht personalisierten zeitweiligen Seriennummer entspricht, die von dem Smartphone eines infizierten Benutzers ausgesendet wird,

11° Testnummer: zufällige Kombination von Einsen und Nullen, die für den Nachweis benutzt wird, dass Sicherheitsschlüssel von einer korrekten App kommen, d.h. einer authentischen Coronalert-App, die auf dem Smartphone des Benutzers zum Zeitpunkt der Anforderung eines Tests installiert ist, ohne dass diese App identifiziert wird,

12° Testcode: Code aus zufälligen Ziffern, der bei einer Testanforderung von der App erstellt wird.

KAPITEL II — *Allgemeines*

Art. 2 - § 1 - Gemäß Artikel 14 § 1 des Zusammenarbeitsabkommens bietet die App folgende Funktionalitäten und führt folgende Einrichtungen aus:

1° Speicherung auf nicht personalisierte Weise der Kontakte des App-Benutzers mit anderen App-Benutzern:

a) Jede App generiert jeden Tag einen neuen Sicherheitsschlüssel.

b) Der Sicherheitsschlüssel ist nur auf dem Smartphone bekannt, auf dem die App installiert ist.

c) Auf der Grundlage des Sicherheitsschlüssels werden nicht personalisierte zeitweilige Seriennummern generiert.

d) Jedes Smartphone, auf dem die App installiert ist, sendet in regelmäßigen Abständen eine nicht personalisierte zeitweilige Seriennummer als Bluetooth-Bake aus; mindestens alle zwanzig Minuten wird eine andere nicht personalisierte zeitweilige Seriennummer ausgesendet, um zu verhindern, dass diese nicht personalisierten zeitweiligen Seriennummern verwendet werden, um einem Benutzer zu folgen; nach Ablauf des Aussenzeitraums werden nicht personalisierte zeitweilige Seriennummern nicht auf dem Smartphone gespeichert, das die Seriennummern ausgesendet hat.

e) Jedes Smartphone, auf dem die App installiert ist, speichert die Bluetooth-Baken mit den nicht personalisierten zeitweiligen Seriennummern, die in kurzer Entfernung befindliche Smartphones aussenden, und Tag des Empfangs der Bake und Stärke des Signals.

f) Die nicht personalisierten zeitweiligen Seriennummern werden auf dem Empfänger-Smartphone während vierzehn Tagen aufbewahrt und anschließend gelöscht.

2° Erstellung und Übertragung eines Testcodes bei Anforderung eines Tests:

a) in geval van symptomen van of risico op besmetting met het coronavirus COVID-19 wordt , in geval een gebruiker van de app zich laat testen, de datum vastgesteld waarop de gebruiker vermoedelijk besmettelijk is geworden; de app genereert een testnummer en berekent de testcode als een éénwegsfunctie van het testnummer en van de datum waarop de gebruiker besmettelijk is geworden;

b) de testcode wordt op initiatief van de gebruiker samen met het identificatienummer van de sociale zekerheid (INSZ) elektronisch aan Sciensano doorgegeven hetzij door de arts die de test voorschrijft, via een softwarepakket, hetzij door de patiënt via een webtoepassing en samen met de datum van de staalafname en de datum waarop de gebruiker besmettelijk is geworden, opgeslagen in Gegevensbank I;

3° Het opvragen van een resultaat van de test:

a) als een resultaat van een test of een ernstig vermoeden van besmetting met het coronavirus COVID-19 beschikbaar is in Gegevensbank I, worden de testcode, de datum van staalafname en de datum waarop de gebruiker besmettelijk is geworden, door Gegevensbank I meegedeeld aan de Gegevensbank VI; na bevestiging van ontvangst van deze gegevens door Gegevensbank VI, wordt de testcode automatisch verwijderd uit Gegevensbank I, waardoor geen connectie meer mogelijk is tussen de gegevens in Gegevensbank I en de gegevens van de app;

b) de app contacteert op geregelde tijdstippen de Gegevensbank VI om na te gaan of er al een resultaat van een test of een ernstig vermoeden van besmetting met het coronavirus COVID-19 beschikbaar is voor de combinatie testcode en datum waarop de gebruiker besmettelijk is geworden; de app kan dus het resultaat van een test bekomen zonder dat de gebruiker geïdentificeerd moet worden;

c) na bevestiging van ontvangst van het resultaat van een test door de app worden het resultaat van de test en de bijhorende testcodes en data verwijderd uit Gegevensbank VI; als het resultaat van een test veertien dagen na de opslag ervan in Gegevensbank VI niet gedownload is, worden het resultaat van de test en de bijhorende testcodes en data verwijderd uit Gegevensbank VI;

d) het testresultaat wordt ten laatste vierentwintig uur na het tonen van het resultaat aan de gebruiker uit de app verwijderd;

e) als de app veertien dagen na de datum van het aanmaken van de testcode nog geen resultaat van de test heeft ontvangen, worden het testnummer, de testcode en de datum waarop de gebruiker besmettelijk is geworden uit de app verwijderd;

4° het doorsturen van de beveiligde sleutels naar Gegevensbank V in geval van een positief resultaat van een test:

a) na ontvangst van een positief resultaat van een test kan de gebruiker toestemming geven om de beveiligde sleutels, het testnummer en de datum waarop hij besmettelijk is geworden, op te laden in Gegevensbank V;

a) en cas de symptômes ou de risque d'infection au coronavirus COVID-19 et lorsqu'un utilisateur de l'appli se fait tester, la date à laquelle l'utilisateur est probablement devenu contagieux est déterminée; l'appli génère un numéro de test et l'appli calcule le code du test comme une fonction à sens unique du numéro de test et de la date à laquelle l'utilisateur est devenu contagieux;

b) le code du test ainsi que le numéro d'identification de la sécurité sociale (NISS) sont transmis, à l'initiative de l'utilisateur, par la voie électronique à Sciensano, soit par le médecin qui prescrit le test, au moyen d'un logiciel, soit par le patient au moyen d'une application web et sont enregistrés dans la Base de données I en même temps que la date du prélèvement et la date à laquelle l'utilisateur est devenu contagieux;

3° La récupération d'un résultat du test:

a) si un résultat d'un test ou une forte présomption d'infection par le coronavirus COVID-19 est disponible dans la Base de données I, le code du test, la date du prélèvement et la date à laquelle l'utilisateur est devenu contagieux, sont communiqués par la Base de données I à la Base de données VI; après confirmation de la réception de ces données par la Base de données VI, le code du test est supprimé automatiquement de la Base de données I, ce qui rend désormais une connexion impossible entre les données de la Base de données I et les données de l'appli;

b) l'appli contacte, à des intervalles réguliers, la Base de données VI afin de vérifier si le résultat d'un test ou une forte présomption d'infection par le coronavirus COVID-19 est déjà disponible pour la combinaison du code de test et de la date à laquelle l'utilisateur est devenu contagieux; l'appli peut donc obtenir le résultat d'un test sans que l'utilisateur ne doive être identifié;

c) après confirmation de la réception du résultat d'un test par l'appli, le résultat du test et les codes de test et données y afférents sont supprimés de la Base de données VI; si le résultat d'un test n'a pas été téléchargé dans les quatorze jours après son enregistrement dans la Base de données VI, le résultat du test et les codes de test et données y afférents sont supprimés de la Base de données VI;

d) le résultat du test est supprimé de l'appli, au plus tard vingt-quatre heures après qu'il ait été montré à l'utilisateur;

e) si l'appli n'a pas encore reçu le résultat du test après quatorze jours à compter de la date de création d'un code de test, le numéro du test, le code du test et la date à laquelle l'utilisateur est devenu contagieux sont supprimés de l'appli;

4° la transmission des clés sécurisées à la Base de données V en cas de résultat de test positif :

a) après réception d'un résultat de test positif, l'utilisateur peut donner l'autorisation pour charger les clés sécurisées, le numéro de test et la date à laquelle il est devenu contagieux dans la Base de données V;

a) Bei Eintreten von Symptomen oder des Risikos einer Infektion mit dem Coronavirus COVID-19 lässt der App-Benutzer sich testen und wird das Datum bestimmt, an dem der Benutzer ansteckend geworden ist; die App generiert eine Testnummer und berechnet den Testcode als Einwegfunktion der Testnummer und des Datums, an dem der Benutzer ansteckend geworden ist.

b) Der Testcode und die Erkennungsnummer der sozialen Sicherheit (NISS) werden auf Initiative des Benutzers elektronisch an Sciensano übermittelt, entweder durch den Arzt, der den Test verschreibt, mittels Software oder durch den Patienten mittels einer Webanwendung, und werden zusammen mit dem Datum der Probeentnahme und dem Datum, an dem der Benutzer ansteckend geworden ist, in der Datenbank I gespeichert;

3° Polling nach Testergebnissen:

a) Ist ein Testergebnis oder ein ernsthafter Verdacht auf eine Infektion mit dem Coronavirus COVID-19 in der Datenbank I verfügbar, übermittelt die Datenbank I der Datenbank VI Testcode, Datum der Probeentnahme und Datum, an dem der Benutzer ansteckend geworden ist; nach Bestätigung des Eingangs dieser Daten in der Datenbank VI wird der Testcode in der Datenbank I automatisch gelöscht; dadurch ist keine Verbindung zwischen den Daten der Datenbank I und den Daten der App mehr möglich.

b) Die App kontaktiert in regelmäßigen Abständen die Datenbank VI, um zu überprüfen, ob für die Kombination Testcode und Datum, an dem der Benutzer ansteckend geworden ist, bereits ein Testergebnis oder ein ernsthafter Verdacht auf eine Infektion mit dem Coronavirus COVID-19 vorliegt; die App kann also ein Testergebnis ohne Identifizierung des Benutzers erhalten.

c) Nach Bestätigung des Empfangs eines Testergebnisses durch die App werden Testergebnis und entsprechende Testcodes und Daten in der Datenbank VI gelöscht; wurde ein Testergebnis nicht innerhalb vierzehn Tagen nach seiner Speicherung in der Datenbank VI heruntergeladen, werden Testergebnis und entsprechende Testcodes und Daten aus der Datenbank VI gelöscht.

d) Das Testergebnis wird spätestens vierundzwanzig Stunden, nachdem es dem Benutzer gezeigt worden ist, aus der App gelöscht.

e) Hat die App nach vierzehn Tagen, zu rechnen ab dem Zeitpunkt der Erstellung eines Testcodes, noch kein Testergebnis erhalten, werden Testnummer, Testcode und Datum, an dem der Benutzer ansteckend geworden ist, aus der App gelöscht.

4° Übertragung der Sicherheitsschlüssel an die Datenbank V bei positivem Testergebnis:

a) Nach Empfang eines positiven Testergebnisses kann der Benutzer erlauben, Sicherheitsschlüssel, Testnummer und Datum, an dem er ansteckend geworden ist, in die Datenbank V hochzuladen.

b) de app verzamelt geen locatiegegevens; de gebruiker kan echter wel binnen de app vrijwillig aangeven in welk(e) land(en) hij op een bepaalde datum is geweest om te kunnen samenwerken met de contactopsporingsapplicaties van andere landen; desgevallend worden de beveiligde sleutels naar het door de gebruiker aangegeven land gestuurd;

c) na bevestiging van ontvangst door Gegevensbank V van de gegevens vermeld onder a) en b), worden het resultaat van de test, de beveiligde sleutels, de lijst van landen, het testnummer, de testcode, en de datum waarop de gebruiker besmettelijk is geworden uit de app verwijderd;

d) op geregelde tijdstippen genereert Gegevensbank V uit de gegevens vermeld onder 4° a) het testnummer en gaat ze na of er een geldige autorisatiecode bestaat voor elke testcode en datum; als aan alle voorwaarden voldaan is, worden de beveiligde sleutels opgenomen in Gegevensbank V;

e) de beveiligde sleutels worden veertien dagen na de datum van ontvangst uit Gegevensbank V verwijderd;

5° Het opsporen van contacten:

a) de app contacteert op geregelde tijdstippen Gegevensbank V en downloadt de sleutels en de bijhorende besmettelijke dagen van alle besmette gebruikers; deze lijst wordt digitaal gedagtekend zodat de app de authenticiteit van deze lijst kan nagaan aan de hand van de publieke sleutel van Gegevensbank V;

b) de app ontcijfert met deze beveiligde sleutels de door deze sleutels gegenereerde niet-gepersonaliseerde tijdelijke serienummers en gaat na of deze serienummers ook opgeslagen zijn in de app; de app berekent op basis van het verschil van de sterkte tussen het verzonden en ontvangen signaal de signaalverzwakking en schat de afstand van het contact in; de totale duur van mogelijke contacten wordt berekend op basis van het aantal serienummers dat overeenkomt; op deze manier kan de app nagaan of in de voorbije veertien dagen een risicocontact heeft plaatsgevonden;

c) als de app een risicocontact detecteert, informeert de app de gebruiker over een mogelijk risico op besmetting met het coronavirus COVID-19.

§ 2. De app laadt op geregelde basis dummy sleutels op in Gegevensbank V. Voor zij dat doet stuurt de app een aantal dummy verzoeken naar Gegevensbank VI, die dummy antwoorden terugstuurt. De dummy sleutels hebben geen geldige autorisatiecode en worden dus niet opgenomen in Gegevensbank V. Op deze manier kan men besmette gebruikers niet onderscheiden van niet-geteste of niet-besmette gebruikers op basis van de communicatiepatronen van de app.

Als er minder dan tien beveiligde sleutels zijn opgeladen op één dag, worden in Gegevensbank V bijkomende dummy beveiligde sleutels opgeladen tot het totaal van tien bereikt wordt.

b) l'appli ne collecte pas de données de localisation; l'utilisateur peut cependant indiquer volontairement dans l'appli le ou les pays dans lesquels il s'est rendu à une date déterminée afin de pouvoir collaborer avec les applications numériques de traçage des contacts d'autres pays; le cas échéant, les clés sécurisées sont envoyées au pays indiqué par l'utilisateur;

c) après confirmation de la réception par la Base de données V des données mentionnées sous a) et b), le résultat du test, les clés sécurisées, la liste de pays, le numéro de test, le code de test et la date à laquelle l'utilisateur est devenu contagieux sont supprimés de l'appli;

d) à des intervalles réguliers, la Base de données V génère, à partir des données mentionnées sous le point 4° a), le numéro de test et elle vérifie s'il existe un code d'autorisation valide pour chaque code de test et chaque date; si toutes les conditions sont remplies, les clés sécurisées sont enregistrées dans la Base de données V;

e) les clés sécurisées sont supprimées de la Base de données V après quatorze jours à compter de leur réception;

5° Le dépistage de contacts:

a) l'appli contacte la Base de données V à des intervalles réguliers et télécharge les clés et les jours contagieux y afférents de l'ensemble des utilisateurs infectés; cette liste est horodatée par la voie numérique de sorte que l'appli puisse vérifier l'authenticité de cette liste au moyen de la clé publique de la Base de données V;

b) l'appli déchiffre avec ces clés sécurisées les numéros de série temporaires non personnalisés générés par ces clés et vérifie si ces numéros de série sont aussi enregistrés dans l'appli; l'appli calcule, sur la base de la différence de puissance entre le signal émis et le signal reçu, l'atténuation du signal et estime la distance du contact; la durée totale des contacts possibles est calculée sur la base du nombre de numéros de série correspondants; l'appli peut donc vérifier de cette manière si un contact à risque a eu lieu au cours des quatorze derniers jours;

c) si l'appli détecte un contact à risque, l'appli informe l'utilisateur sur un risque possible d'infection par le coronavirus COVID-19.

§ 2. L'appli charge, à des intervalles réguliers, des clés fictives dans la base de données V. Préalablement à cela, l'appli envoie plusieurs requêtes fictives à la Base de données VI, qui renvoie des réponses fictives. Les clés fictives n'ont pas de code d'autorisation valable et ne sont donc pas chargées dans la Base de données V. De cette manière, il est impossible de distinguer, sur la base des modèles de communication de l'appli, les utilisateurs infectés des utilisateurs non testés ou non infectés.

Si moins de dix clés sécurisées ont été chargées en un jour, des clés sécurisées fictives supplémentaires sont ajoutées dans la Base de données V pour en obtenir au total dix.

b) Die App sammelt keine Lokalisierungsdaten; der Benutzer kann jedoch freiwillig in der App angeben, in welchem Land/in welchen Ländern er zu einem bestimmten Zeitpunkt war, um eine Zusammenarbeit mit digitalen Kontaktrückverfolgungsanwendungen anderer Länder zu ermöglichen; gegebenenfalls werden die Sicherheitsschlüssel an das vom Benutzer angegebene Land geschickt.

c) Nach Bestätigung des Eingangs der unter Buchstabe a) und b) erwähnten Daten durch die Datenbank V werden Testergebnis, Sicherheitsschlüssel, Liste der Länder, Testnummer, Testcode und Datum, an dem der Benutzer ansteckend geworden ist, aus der App gelöscht.

d) In regelmäßigen Abständen überprüft die Datenbank V, ob eingegangene Testnummern mit den Testcodes und Daten, an denen Benutzer ansteckend geworden sind, übereinstimmen und ob für jeden Testcode und jedes Datum ein Ermächtigungscode besteht; sind alle Bedingungen erfüllt, werden die Sicherheitsschlüssel in der Datenbank V gespeichert.

e) Sicherheitsschlüssel werden nach vierzehn Tagen, zu rechnen ab ihrem Eingang, in der Datenbank V gelöscht.

5° Kontaktermittlung

a) Die App kontaktiert in regelmäßigen Abständen die Datenbank V und lädt die Sicherheitsschlüssel und die diesbezüglichen Tage mit Ansteckungsgefahr der gesamten infizierten Benutzer herunter; diese Liste wird digital unterzeichnet; somit kann die App anhand des öffentlichen Schlüssels der Datenbank V die Echtheit dieser Liste überprüfen.

b) Mit diesen Sicherheitsschlüsseln entziffert die App die mit diesen Schlüsseln generierten nicht personalisierten zeitweiligen Seriennummern und überprüft, ob diese Seriennummern auch in der App gespeichert sind; die App berechnet auf der Grundlage des Unterschieds der Signalstärke zwischen ausgesendetem Signal und empfangenem Signal die Signalschwächung und schätzt den Kontaktabstand; die Gesamtdauer der möglichen Kontakte wird auf der Grundlage der Anzahl übereinstimmender Seriennummern berechnet; auf diese Weise kann die App überprüfen, ob in den letzten vierzehn Tagen ein Risikokontakt stattgefunden hat.

c) Wenn die App einen Risikokontakt erkennt, informiert sie den Benutzer über das mögliche Risiko einer Infektion mit dem Coronavirus COVID-19.

§ 2 - Die App lädt in regelmäßigen Abständen fiktive Schlüssel in die Datenbank V hoch. Zuvor sendet de App mehrere fiktive Abfragen an die Datenbank VI, die fiktive Antworten zurücksendet. Fiktive Schlüssel haben keinen gültigen Ermächtigungscode und werden daher nicht in die Datenbank V hochgeladen. Auf diese Weise ist es unmöglich, auf der Grundlage der Kommunikationsmodelle der App infizierte Benutzer von nicht getesteten oder nicht infizierten Benutzern zu unterscheiden.

Sind an einem Tag weniger als zehn Sicherheitsschlüssel hochgeladen worden, werden zusätzliche fiktive Schlüssel in die Datenbank V hochgeladen, um die Zahl von zehn Schlüsseln zu erreichen.

HOOFDSTUK III. — *Technische specificaties en interoperabiliteit*

Art. 3. De app wordt aangeboden op iOS en Android.

Art. 4. §1. De app moet :

1° eenvoudig te installeren en te gebruiken zijn;

2° werken met een beperkt batterijverbruik;

3° voldoende nauwkeurig zijn; dit betekent dat de app enkel contacten van minstens vijftien minuten binnen een afstand van minder dan twee meter als risicocontact detecteert;

4° internationale interoperabiliteit ondersteunen en het Bluetooth-gedeelte van de app in een zo groot aantal mogelijk landen bruikbaar maken door dit gedeelte compatibel te maken met de apps gebruikt in de meeste EU landen.

§ 2. De Gegevensbank V en de Gegevensbank VI, en de daarvoor gebruikte infrastructuur moet:

1° een goede performantie leveren, schaalbaar zijn voor gebruik door meerdere miljoenen gebruikers en bestand zijn tegen aanvallen;

2° de mogelijkheid bieden om de beveiligde sleutels uit te wisselen met andere landen binnen de EU en dit rechtstreeks of via de EU Federation Gateway Service ; beveiligde sleutels worden enkel verstuurd naar de tegenhanger van Gegevensbank V van dat land of regio als:

a) dat land of regio een gedecentraliseerde contactopsporingsapp heeft, erkend door de nationale of regionale gezondheidsdienst met een Bluetooth gedeelte dat compatibel is met de Belgische app;

b) er voldoende waarborgen zijn voor de gegevensbescherming met inbegrip van de veilige communicatie tussen Gegevensbank V en haar tegenhanger;

c) de gebruiker van de app heeft aangegeven dat hij/zij dat land of die regio bezocht heeft in de periode waarin hij/zij besmettelijk was. Voor het ontvangen van beveiligde sleutels uit andere landen of regio's gelden voorwaarden a) en b);

d) de beveiligde sleutel van het buitenland afkomstig is van een gebruiker die aangegeven heeft dat hij/zij België bezocht heeft in de periode waarin hij/zij besmettelijk was. Nadat de beveiligde sleutels zijn aangekomen in Gegevensbank V of in de tegenhanger ervan in een ander land of regio, worden ze gedownload in de apps van het land of de regio;

3° valse of incorrecte rapportering van besmettingen vermijden; de rapportering van een besmetting kan enkel na een positief resultaat van een test of na een vaststelling door een arts van een ernstig vermoeden dat een persoon besmet is met het coronavirus COVID-19;

4° dermate zijn opgezet dat er geen relatie kan gelegd worden tussen berichten, zoals beveiligde sleutels en testresultaten en IP-adressen van gebruikers.

§3. De app en de serverinfrastructuur moeten de persoonlijke levenssfeer van de gebruikers waarborgen, gebaseerd zijn op minimale gegevensverwerking en gegevensbescherming door ontwerp. Dit houdt onder meer in dat:

CHAPITRE III. — *Spécifications techniques et interoperabilité*

Art. 3. L'appli est offerte sur iOS et Android.

Art. 4. § 1^{er}. L'appli doit:

1° être simple à installer et à utiliser;

2° fonctionner avec une consommation de batterie réduite;

3° être suffisamment précise; cela signifie que l'appli détecte uniquement les contacts d'au moins quinze minutes à une distance de moins de deux mètres comme étant des contacts à risque;

4° soutenir l'interopérabilité internationale et rendre la partie Bluetooth de l'appli exploitable dans un maximum de pays en rendant cette partie compatible avec les applis utilisées dans la plupart des pays de l'UE.

§ 2. La Base de données V et la Base de données VI et l'infrastructure utilisée à cet effet doivent:

1° assurer une bonne performance, être échelonnables en vue d'une utilisation par plusieurs millions de personnes et pouvoir résister à des attaques;

2° offrir la possibilité d'échanger les clés sécurisées avec d'autres pays au sein de l'UE, et ce directement ou via le Federation Gateway Service de l'UE; les clés sécurisées sont uniquement envoyées au pendant de la Base de données V de ce pays ou de cette région si:

a) ce pays ou cette région possède une appli de traçage des contacts décentralisée, reconnue par le service sanitaire national ou régional, se composant d'une partie Bluetooth qui est compatible avec l'appli belge;

b) il y a suffisamment de garanties pour la protection des données, en ce compris une communication sécurisée entre la Base de données V et son pendant;

c) l'utilisateur de l'appli a indiqué qu'il a visité ce pays ou cette région durant la période au cours de laquelle il était contagieux. S'applique à la réception de clés sécurisées provenant d'autres pays ou régions, les conditions a) et b);

d) la clé sécurisée de l'étranger provient d'un utilisateur qui a indiqué qu'il a visité la Belgique durant la période au cours de laquelle il était contagieux. Après que les clés sécurisées sont arrivées dans la Base de données V ou dans son pendant dans un autre pays ou une autre région, elles sont téléchargées dans les applis du pays ou de la région.

3° éviter un faux rapportage ou un rapportage incorrect d'infections; le rapportage d'une infection n'est possible qu'après un résultat de test positif ou après une constatation par un médecin d'une présomption sérieuse d'infection par le coronavirus COVID-19;

4° être conçues de la sorte qu'il ne soit pas possible d'établir de relation entre les messages, comme les clés sécurisées et les résultats de test et les adresses IP des utilisateurs.

§3. L'appli et l'infrastructure du serveur doivent garantir le respect de la vie privée des utilisateurs, doivent être basées sur la minimisation des données et la protection des données dès la conception. Cela signifie notamment que:

KAPITEL III — *Technische Spezifikationen und Interoperabilität*

Art. 3 - Die App wird für iOS und Android angeboten.

Art. 4 - § 1 - Die App muss:

1. leicht zu installieren und zu benutzen sein,

2. mit geringem Batterieverbrauch arbeiten,

3. ausreichend präzise sein; das bedeutet, dass die App nur Kontakte von mindestens fünfzehn Minuten mit einem Abstand von weniger als zwei Metern als Risikokontakte erkennt,

4. die internationale Interoperabilität unterstützen und den Bluetooth-Teil der App in möglichst vielen Ländern nutzbar machen, indem dieser Teil mit den in den meisten EU-Ländern verwendeten Apps kompatibel gemacht wird.

§ 2 - Die Datenbank V und die Datenbank VI und die dafür benutzte Infrastruktur müssen:

1° eine gute Leistungsfähigkeit aufweisen, für die Benutzung durch mehrere Millionen Benutzer skalierbar sein und Angriffen standhalten können,

2° die Möglichkeit bieten, Sicherheitsschlüssel mit anderen EU-Ländern entweder direkt oder über das EU-Portal auszutauschen; die Sicherheitsschlüssel werden nur dann an das Pendant der Datenbank V dieses Landes oder dieser Region gesendet, wenn:

a) dieses Land oder diese Region über eine dezentralisierte, vom nationalen oder regionalen Gesundheitsdienst anerkannte App zur Kontaktrückverfolgung verfügt, die aus einem Bluetooth-Teil besteht, der mit der belgischen App kompatibel ist;

b) es ausreichende Garantien für den Datenschutz gibt, einschließlich einer sicheren Kommunikation zwischen der Datenbank V und ihrem Pendant;

c) der Benutzer der App angegeben hat, dass er dieses Land oder diese Region während des Zeitraums, in dem er ansteckend war, besucht hat. Für den Empfang von Sicherheitsschlüsseln aus anderen Ländern oder Regionen gelten die Bedingungen a) und b);

d) der Sicherheitsschlüssel aus dem Ausland stammt von einem Benutzer, der angegeben hat, dass er Belgien während des Zeitraums, in dem er ansteckend war, besucht hat. Nachdem die Sicherheitsschlüssel in der Datenbank V oder ihrem Pendant in einem anderen Land oder einer anderen Region eingetroffen sind, werden sie in die Apps des Landes oder der Region hochgeladen.

3° falsche oder fehlerhafte Meldungen von Infektionen vermeiden; die Meldung einer Infektion ist nur nach einem positiven Testergebnis oder nach Feststellung eines ernsthaften Verdachts auf eine Infektion mit dem Coronavirus COVID-19 durch einen Arzt möglich,

4° so gestaltet sein, dass es nicht möglich ist, eine Verbindung zwischen Nachrichten, wie Sicherheitsschlüssel und Testergebnisse, und den IP-Adressen der Benutzer herzustellen.

§ 3 - App und Serverinfrastruktur müssen die Achtung vor dem Privatleben der Benutzer gewährleisten und auf Datenminimierung und Datenschutz durch Technikgestaltung gestützt sein. Dies beinhaltet unter anderem, dass:

1° er geen locatie-informatie mag ingezameld worden;

2° alle communicatie tussen de app en de gegevensbanken gecijferd wordt;

3° er geen informatie wordt verwerkt over wie waar door wie besmet is;

4° er geen beveiligde sleutels worden verzameld van een gebruiker die niet besmet is;

5° het systeem uitgeschakeld zal worden en alle opgeslagen informatie verwijderd zal worden ten laatste vijf dagen na de publicatie van het koninklijk besluit dat het einde van de toestand van de coronavirus COVID-19 epidemie afkondigt;

6° bij uitwisseling van gegevens naar Gegevensbanken I en V en naar de Gegevensbank VI slechts het minimum aan gegevens mag uitgewisseld worden om het resultaat van de test te kunnen sturen naar de juiste app, zodat de kans op identificatie van de betrokkene minimaal gehouden wordt;

7° het niet mogelijk is om het systeem of de gegevens voor andere doeleinden te gebruiken.

§ 4. De werking van het systeem voorziet in minimale administratieve lasten middels een eenvoudige ingave van de testcode bij het aanvragen van een test.

HOOFDSTUK IV. — Informatieverplichting

Art. 5. § 1. De gebruikers worden, bij de installatie en voor het gebruik ervan, geïnformeerd over de werking van de app en de interactie ervan met de Gegevensbanken I, V en VI.

Hiertoe wordt op de website www.coronalert.be alle nuttige informatie over de app en de gegevensbanken gepubliceerd, onder meer de functionaliteiten, de werking, het charter, de privacyverklaring en de gegevensbeschermingseffectbeoordeling. De app zelf bevat ook verwijzingen naar informatie over de functionaliteiten, de werking en de privacyverklaring.

§ 2. De broncode van de app en van de programma's voor het beheer van de Gegevensbank V en de Gegevensbank VI in het bijzonder de onderdelen die de gegevens voor een test genereren, de resultaten van een test downloaden, de beveiligde sleutels opladen en het risico berekenen, evenals de gebruikersinterface van de app, worden aan de hand van een link publiek gemaakt op de website, bedoeld in §1, eerste lid.

HOOFDSTUK V. — Controle

Art. 6. De werking en de noodzaak van de app wordt regelmatig gemonitord, geëvalueerd en bijgesteld onder aansturing van het Interfederaal Comité Testing en Tracing, bestaande uit vertegenwoordigers van de gefedereerde entiteiten, Sciensano, het eHealth-platform en twee wetenschappelijke experts. Dit comité kan ondersteund worden door een interdisciplinaire werkgroep van wetenschappelijke experts.

De app zal tevens het voorwerp uitmaken van een informatieveiligheidsaudit door een instantie onafhankelijk van diegene die de app ontwikkeld heeft, waarbij onder meer wordt nagegaan of deze beantwoordt aan de informatieveiligheidsvoorwaarden en in overeenstemming is met de geldende regelgeving.

1° aucune donnée de localisation ne peut être collectée;

2° l'ensemble des communications entre l'appli et les bases de données doivent être chiffrées;

3° aucune donnée n'est traitée concernant qui est infecté à quel endroit et par quelle personne;

4° aucune clé sécurisée n'est collectée pour un utilisateur qui n'est pas infecté;

5° le système sera arrêté et toutes les informations enregistrées seront supprimées au plus tard cinq jours après le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie du coronavirus COVID-19;

6° lors de l'échange de données avec les Bases de données I et V et avec la Base de données VI, seul le minimum de données peut être échangé pour pouvoir envoyer le résultat du test à l'appli correcte de sorte que le risque d'identification de la personne concernée soit réduit au minimum;

7° il n'est pas possible d'utiliser le système ou les données pour d'autres finalités.

§ 4. Le fonctionnement du système prévoit des formalités administratives minimales grâce à une introduction aisée du code du test lors de la demande d'un test.

CHAPITRE IV. — Obligation d'information

Art. 5. 1^{er}. Lors de son installation et avant son utilisation, les utilisateurs sont informés sur le fonctionnement de l'appli et son interaction avec les Bases de données I, V et VI.

À cet effet, seront publiées sur le site www.coronalert.be toutes les informations utiles sur l'appli et les bases de données, en ce compris les fonctionnalités, le fonctionnement, la charte, la déclaration de vie privée et l'analyse d'impact relative à la protection des données. L'appli contient elle-même aussi des références aux informations concernant les fonctionnalités, le fonctionnement et la déclaration de vie privée.

§ 2. Le code source de l'appli et des programmes de gestion de la Base de données V et de la Base de données VI, en particulier les composants qui génèrent les données pour un test, téléchargent les résultats d'un test, chargent les clés sécurisées et calculent le risque, ainsi que l'interface utilisateur de l'appli, seront rendus publics au moyen d'un lien sur le site internet visé au §1^{er}, alinéa 1^{er}.

CHAPITRE V. — Contrôle

Art. 6. Le fonctionnement et la nécessité de l'appli sont régulièrement contrôlés, évalués et rectifiés sous l'impulsion du Comité interfédéral de testing et tracing qui se compose de représentants d'entités fédérées, de Sciensano, de la Plate-forme eHealth et de deux experts scientifiques. Ce comité peut être soutenu par un groupe de travail interdisciplinaire d'experts scientifiques.

L'appli fera également l'objet d'un audit de la sécurité de l'information par une instance indépendante de celle qui a développé l'appli, qui permettra notamment de vérifier si cette appli satisfait aux conditions en matière de sécurité de l'information et est conforme à la réglementation en vigueur.

1° keine Lokalisierungsdaten benutzt werden dürfen,

2° die gesamte Kommunikation zwischen der App und den Datenbanken verschlüsselt sein muss,

3° keinerlei Daten verarbeitet werden in Bezug auf wer wo von wem infiziert worden ist,

4° keinerlei Sicherheitsschlüssel gesammelt wird für einen nicht infizierten Benutzer,

5° das System gestoppt wird und alle gespeicherten Informationen spätestens fünf Tage nach Veröffentlichung des Königlichen Erlasses zur Erklärung der Beendigung des Zustands der Epidemie des Coronavirus COVID-19 gelöscht werden,

6° bei Austausch von Daten der Gesundheitsinfrastruktur mit den Datenbanken I und V und mit der Datenbank VI nur ein Minimum an Daten ausgetauscht werden darf, damit das Risiko auf Identifizierung des Betroffenen auf ein Minimum reduziert wird,

7° es nicht möglich ist, das System oder die Daten für andere Zwecke zu benutzen.

§ 4 - Die Integration mit der Gesundheitsinfrastruktur ermöglicht eine Reduzierung der Gemeinkosten auf ein Minimum bei Anforderung eines Tests.

KAPITEL IV — Informationspflicht

Art. 5 - § 1 - Benutzer werden während der Installation und vor dem Gebrauch über die Funktionsweise der App und ihre Interaktion mit den Datenbanken I, V und VI informiert.

Zu diesem Zweck werden auf der Website www.coronalert.be alle nützlichen Informationen über die App und die Datenbanken veröffentlicht, darin einbegriffen Funktionalitäten, Funktionsweise, Charta, Datenschutzerklärung und Datenschutz-Folgenabschätzung. Die App selbst enthält auch Verweise nach den Informationen über Funktionalitäten, Funktionsweise und Datenschutzerklärung.

§ 2 - Der Quellcode der App und der Verwaltungsprogramme für die Datenbank V und die Datenbank VI werden veröffentlicht, insbesondere die Komponenten, die die Daten für einen Test generieren, die Ergebnisse eines Tests herunterladen, die Sicherheitsschlüssel hochladen und das Risiko berechnen, und die Benutzeroberfläche der App.

KAPITEL V — Kontrolle

Art. 6 - Der Betrieb der App wird regelmäßig kontrolliert, beurteilt und angepasst auf Anregung des Interföderalen Ausschusses Testing und Tracing, der sich aus Vertretern der föderierten Teilgebiete, von Sciensano und der eHealth-Plattform und zwei wissenschaftlichen Sachverständigen zusammensetzt. Dieser Ausschuss kann von einer interdisziplinären Arbeitsgruppe wissenschaftlicher Sachverständiger beigegeben werden.

Die App wird auch einem Informationssicherheitsaudit durch eine vom Anwendungsentwickler unabhängige Stelle unterzogen werden; bei diesem Audit wird unter anderem überprüft, ob die App die Anforderungen an die Informationssicherheit erfüllt und den geltenden Vorschriften entspricht.

HOOFDSTUK VI. — *Inwerkingtreding*

Art. 7. Dit akkoord treedt in werking op dezelfde dag als het samenwerkingsakkoord, in uitvoering waarvan het wordt gesloten.

Opgemaakt te Brussel, in negen exemplaren waarvan elke partij verklaart er één te hebben ontvangen, op 13 oktober 2020.

De Eerste Minister,
A. DE CROO

De vice-eerste Minister en Minister van
Sociale Zaken en Volksgezondheid,
F. VANDENBROUCKE

De Minister-President van de Vlaamse Rege-
ring en Vlaams Minister van Buitenlandse
Zaken, Cultuur, ICT en Facilitair Manage-
ment van de Vlaamse Regering,
J. JAMBON

De Vlaams Minister van Welzijn, Volksgezond-
heid, Gezin en Armoedebestrijding van de
Vlaamse Regering,
W. BEKE

De Minister-President
van de Waalse Regering,
E. DI RUPO

De Vice-Minister-President en Minister van
Werk, Vorming, Gezondheid, Sociale Actie,
Gelijke Kansen en Vrouwenrechten van de
Waalse Regering,
C. MORREALE

De Vice-Minister-President en Minister van
Economie, Buitenlandse Handel, Onder-
zoek en Innovatie, Digitale technologieën,
Landbouw, Ruimtelijke Ordening, het "IFAP-
ME" en de Vaardigheidscentra van de Waalse
Regering,
W. BORSUS

De Minister-President, Minister van Lokale
Besturen en Financiën van de Regering van
de Duitstalige Gemeenschap
O. PAASCH

De Vice-Minister-President en Minister van
Gezondheid en Sociale Aangelegenheden,
Ruimtelijke Ordening en Huisvesting van
de Regering van de Duitstalige Gemeen-
schap,
A. ANTONIADIS

De Voorzitter van het Verenigd College van de
Gemeenschappelijke Gemeenschapscommis-
sie,
R. VERVOORT

Het lid van het Verenigd College van de
Gemeenschappelijke Gemeenschapscommis-
sie, belast met Gezondheid en Welzijn
A. MARON

Het lid van het Verenigd College van de
Gemeenschappelijke Gemeenschapscommis-
sie, belast met Gezondheid en Welzijn
E. VAN DEN BRANDT

CHAPITRE VI. — *Entrée en vigueur*

Art. 7. Le présent accord entre en vigueur le même jour que l'accord de coopération en exécution duquel il a été conclu.

Établi à Bruxelles, en neuf exemplaires, dont chaque partie déclare en avoir reçu un, le 13 octobre 2020.

Le Premier Ministre,
A. DE CROO

Le Vice-Premier Ministre et Ministre des
Affaires sociales et de la Santé publique,
F. VANDENBROUCKE

Le Ministre-Président du Gouvernement flam-
mand et Ministre flamand de la Politique
extérieure, de la Culture, la TI et les Services
généraux,
J. JAMBON

Le Ministre flamand du Bien-Être, de la Santé
publique, de la Famille et de la Lutte contre
la Pauvreté,
W. BEKE

Le Ministre-Président
du Gouvernement wallon,
E. DI RUPO

La Vice-Présidente et Ministre de l'Emploi, de
la Formation, de la Santé, de l'Action sociale,
de l'Égalité des chances et des Droits des
femmes du Gouvernement wallon,
C. MORREALE

Le Vice-Président et Ministre de l'Économie,
du Commerce extérieur, de la Recherche et
de l'Innovation, du Numérique, de l'Agric-
ulture, de l'Aménagement du territoire, de
l'IFAPME et des Centres de compétence du
Gouvernement wallon,
W. BORSUS

Le Ministre-Président, Ministre des Pouvoirs
locaux et des Finances du gouvernement de
la Communauté Germanophone
O. PAASCH

Le Vice-Ministre-Président et Ministre de la
Santé et des Affaires sociales, de l'Aména-
gement du territoire et du Logement de la
Communauté germanophone,
A. ANTONIADIS

Le Président du Collège réuni
de la Commission communautaire commune,
R. VERVOORT

Le membre du Collège réuni de la Commis-
sion communautaire commune, ayant la
Santé et l'Action sociale dans ses attribu-
tions
A. MARON

Le membre du Collège réuni de la Commis-
sion communautaire commune, ayant la
Santé et l'Action sociale dans ses attribu-
tions
E. VAN DEN BRANDT

KAPITEL VI — *Inkrafttreten*

Art. 7 - Vorliegendes Abkommen tritt am selben Tag in Kraft wie das Zusammenarbeitsabkommen, in dessen Ausführung es abgeschlossen worden ist.

In Brüssel in neun Exemplaren aufgestellt, von denen jede Vertragspartei erklärt, eines erhalten zu haben, am Ausgestellt in Brüssel, am 13. Oktober 2020, in einer Originalausfertigung.

Der Premierminister
A. DE CROO

Der Minister der Sozialen Angelegenheiten
und der Volksgesundheits
F. VANDENBROUCKE

Ministerpräsident und Flämischer Minister
für Auswärtige Angelegenheiten, Kultur,
IKT und Facility Management
J. JAMBON

Der Minister des Wohlbefindens, der Volksge-
sundheit, der Familie und der Armutsbe-
kämpfung
W. BEKE

Für die Wallonische Region
Der Minister-Präsident
E. DI RUPO

Die Vizepräsidentin und Ministerin für Beschäf-
tigung, Ausbildung, Gesundheit, soziale
Maßnahmen, Chancengleichheit und Rechte
der Frauen
C. MORREALE

Der Vizepräsident und Minister für Wirtschaft,
Außenhandel, Forschung und Innovation,
digitale Technologien, Raumordnung, Land-
wirtschaft, das IFAPME und die Kompetenzz-
entren
W. BORSUS

Der Minister-President, Ministerpräsident,
Minister für lokale Behörden und Finanzen
O. PAASCH

Der Vize-Ministerpräsident, Minister für
Gesundheit und Soziales, Raumordnung und
Wohnungswesen
A. ANTONIADIS

Der Präsident des Vereinigten Kollegiumss
R. VERVOORT

Das für die Soziale Aktion und die Gesundheit
und das Wohlbefinden zuständige Mitglied
des Vereinigten Kollegiums
A. MARON

Das für die Soziale Aktion und die Gesundheit
und das Wohlbefinden zuständige Mitglied
des Vereinigten Kollegiums
E. VAN DEN BRANDT