Verfassungsgerichtshof

Entscheid Nr. 110/2022
vom 22. September 2022
Geschäftsverzeichnisnrn. 7555, 7556, 7557, 7558, 7559 und 7560

In Sachen: Klagen auf Nichtigerklärung des Dekrets der Wallonischen Region vom 30. September 2020, des Dekrets der Deutschsprachigen Gemeinschaft vom 12. Oktober 2020, von Artikel 2 des Gesetzes vom 9. Oktober 2020, der Ordonnanz der Gemeinsamen Gemeinschaftskommission vom 1. Oktober 2020 und des Dekrets der Flämischen Gemeinschaft vom 2. Oktober 2020 « zur Billigung 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, Gesundheitsinspektionsdienste und mobilen Teams im Rahmen einer Kontaktermittlung bei (vermutlich) mit dem Coronavirus COVID-19 infizierten Personen auf der Grundlage einer Datenbank bei Sciensano », erhoben von der VoG « Vivant Ostbelgien » und anderen und von der VoG « Ligue des droits humains ».

Der Verfassungsgerichtshof,

zusammengesetzt aus den Präsidenten P. Nihoul und L. Lavrysen, den Richtern T. Giet, J. Moerman, M. Pâques, Y. Kherbache, T. Detienne, D. Pieters, S. de Bethune, E. Bribosia und W. Verrijdt, und dem emeritierten Richter J.-P. Moerman gemäß Artikel 60*bis* des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, unter Assistenz des Kanzlers P.-Y. Dutilleux, unter dem Vorsitz des Präsidenten P. Nihoul,

erlässt nach Beratung folgenden Entscheid:

I. *Gegenstand der Klagen und Verfahren*

a. Mit einer Klageschrift, die dem Gerichtshof mit am 12. April 2021 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 14. April 2021 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung des Dekrets der Wallonischen Region vom 30. September 2020 « zur Billigung 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,

Gesundheitsinspektionsdienste und mobilen Teams im Rahmen einer Kontaktermittlung bei (vermutlich) mit dem Coronavirus COVID-19 infizierten Personen auf der Grundlage einer Datenbank bei Sciensano » (veröffentlicht im *Belgischen Staatsblatt* vom 15. Oktober 2020, zweite Ausgabe): die VoG « Vivant Ostbelgien », Diana Stiel, Alain Mertes und Michael Balter, unterstützt und vertreten durch RA R. Fonteyn, in Brüssel zugelassen.

b. Mit einer Klageschrift, die dem Gerichtshof mit am 12. April 2021 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 14. April 2021 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung des Dekrets der Deutschsprachigen Gemeinschaft vom 12. Oktober 2020 « zur Billigung 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, Gesundheitsinspektionsdienste und mobilen Teams im Rahmen einer Kontaktermittlung bei (vermutlich) mit dem Coronavirus COVID-19 infizierten Personen auf der Grundlage einer Datenbank bei Sciensano » (veröffentlicht im *Belgischen Staatsblatt* vom 15. Oktober 2020, zweite Ausgabe): die VoG « Vivant Ostbelgien », Diana Stiel, Alain Mertes und Michael Balter, unterstützt und vertreten durch RA R. Fonteyn.

c. Mit Klageschriften, die dem Gerichtshof mit am 12. April 2021 bei der Post aufgegebenen Einschreibebriefen zugesandt wurden und am 14. April 2021 in der Kanzlei eingegangen sind, erhoben Klage auf Nichtigerklärung von Artikel 2 des Gesetzes vom 9. Oktober 2020 « zur Billigung 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, Gesundheitsinspektionsdienste und mobilen Teams im Rahmen einer Kontaktermittlung bei (vermutlich) mit dem Coronavirus COVID-19 infizierten Personen auf der Grundlage einer Datenbank bei Sciensano » (veröffentlicht im *Belgischen Staatsblatt* vom 15. Oktober 2020, zweite Ausgabe): die VoG « Ligue des droits humains », unterstützt und vertreten durch RÄin C. Forget, RÄin S. Najmi, in Brüssel zugelassen, und RA R. Fonteyn, und die VoG « Vivant Ostbelgien », Diana Stiel, Alain Mertes und Michael Balter, unterstützt und vertreten durch RA R. Fonteyn.

d. Mit einer Klageschrift, die dem Gerichtshof mit am 12. April 2021 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 14. April 2021 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung der Ordonnanz der Gemeinsamen Gemeinschaftskommission vom 1. Oktober 2020 « zur Billigung 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, Gesundheitsinspektionsdienste und mobilen Teams im Rahmen einer Kontaktermittlung bei (vermutlich) mit dem Coronavirus COVID-19 infizierten Personen auf der Grundlage einer Datenbank bei Sciensano » (veröffentlicht im *Belgischen Staatsblatt* vom 15. Oktober 2020, zweite Ausgabe): die VoG « Vivant Ostbelgien », Diana Stiel, Alain Mertes und Michael Balter, unterstützt und vertreten durch RA R. Fonteyn.

e. Mit einer Klageschrift, die dem Gerichtshof mit am 12. April 2021 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 14. April 2021 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung des Dekrets der Flämischen Gemeinschaft vom 2. Oktober 2020 « zur Billigung 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, Gesundheitsinspektionsdienste und mobilen Teams im Rahmen einer Kontaktermittlung bei (vermutlich) mit dem Coronavirus COVID-19 infizierten Personen auf der Grundlage einer Datenbank bei Sciensano » (veröffentlicht im *Belgischen Staatsblatt* vom 15. Oktober 2020, zweite Ausgabe): die VoG « Vivant Ostbelgien », Diana Stiel, Alain Mertes und Michael Balter, unterstützt und vertreten durch RA R. Fonteyn.

Diese unter den Nummern 7555, 7556, 7557, 7558, 7559 und 7560 ins Geschäftsverzeichnis des Gerichtshofes eingetragenen Rechtssachen wurden verbunden.

Schriftsätze und Gegenerwiderungsschriftsätze wurden eingereicht von

- dem Ministerrat, unterstützt und vertreten durch RÄin M. Feys, in Gent zugelassen,

- der Flämischen Regierung, unterstützt und vertreten durch RÄin M. Feys,

- der Wallonischen Regierung, unterstützt und vertreten durch RÄin M. Feys;

- dem Vereinigten Kollegium der Gemeinsamen Gemeinschaftskommission, unterstützt und vertreten durch RÄin M. Feys,

- der Regierung der Deutschsprachigen Gemeinschaft, unterstützt und vertreten durch RÄin M. Feys.

Die klagenden Parteien in den Rechtssachen Nrn. 7555, 7556, 7558, 7559 und 7560 haben einen Erwiderungsschriftsatz eingereicht.

Durch Anordnung vom 18. Mai 2022 hat der Gerichtshof nach Anhörung der referierenden Richter T. Detienne und W. Verrijdt

- beschlossen, dass die Rechtssachen verhandlungsreif sind und den Sitzungstermin auf den 29. Juni 2022 anberaumt,

- die Parteien aufgefordert, vorher die folgenden Fragen durch einen Ergänzungsschriftsatz zu beantworten, der spätestens am 17. Juni 2022 durch einen bei der Post aufgegebenem Einschreibebrief einzureichen und innerhalb derselben Frist den anderen Parteien sowie der Kanzlei des Gerichtshofs per E-Mail an die Adresse « griffie@const-court.de » zu übermitteln ist:

« 1. Können Sie den Zusammenhang von Artikel 6 §§ 5 und 6, von Artikel 7 und von Artikel 10 § 1 des Zusammenarbeitsabkommens vom 25. August 2020 erklären? Warum sind

bestimmte Datenkategorien der Datenbank I, die gemäß Artikel 6 §§ 5 und 6 des Zusammenarbeitsabkommens vom 25. August 2020 von den Kontaktzentren Sciensano mitgeteilt werden, identisch mit dem Datenkategorien der Datenbank III, die gemäß Artikel 7 von Sciensano den Kontaktzentren mitgeteilt werden?

2. Wie werden die in Artikel 6 §§ 5 und 6 des Zusammenarbeitsabkommens erwähnten personenbezogenen Daten von den Kontaktzentren Sciensano im Hinblick auf ihre Erfassung in der Datenbank I mitgeteilt? Erfassen die Kontaktzentren in der Datenbank I die Daten, die sie erheben, und falls ja, auf der Grundlage welcher Bestimmung?

3. Können Sie die Bezugnahme in Artikel 3 § 1 Nr. 4 und in Artikel 10 § 2 des Zusammenarbeitsabkommens vom 25. August 2020 auf die ‘ in Artikel 6 erwähnten ’ Personen der Kategorien V und/oder VI erläutern? Werden die personenbezogenen Daten der Personen der Kategorien V und VI in der Datenbank I gesammelt und falls ja, auf der Grundlage welcher Bestimmung? ».

Ergänzungsschriftsätze wurden eingereicht von

- dem Ministerrat,

- der Flämischen Regierung,

- der Wallonischen Regierung,

- dem Vereinigten Kollegium der Gemeinsamen Gemeinschaftskommission,

- der Regierung der Deutschsprachigen Gemeinschaft.

Auf der öffentlichen Sitzung vom 29. Juni 2022

- erschienen

. RA R. Fonteyn, für die klagenden Parteien in den Rechtssachen Nrn. 7555, 7556, 7558, 7559 und 7560,

. Me R. Fonteyn, ebenfalls *loco* RÄin C. Forget und RÄin S. Najmi, für die klagende Partei in der Rechtssache Nr. 7557,

. RÄin M. Feys und RA A. Vandeburie, in Brüssel zugelassen, für den Ministerrat, die Flämische Regierung, die Wallonische Regierung, das Vereinigte Kollegium der Gemeinsamen Gemeinschaftskommission und die Regierung der Deutschsprachigen Gemeinschaft,

- haben die referierenden Richter T. Detienne und W. Verrijdt Bericht erstattet,

- wurden die vorgenannten Rechtsanwälte angehört,

- wurden die Rechtssachen zur Beratung gestellt.

Die Vorschriften des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, die sich auf das Verfahren und den Sprachengebrauch beziehen, wurden zur Anwendung gebracht.

II. *Rechtliche Würdigung*

(…)

In Bezug auf den Kontext der angefochtenen Akte

B.1.1. Die klagenden Parteien beantragen die Nichtigerklärung des Dekrets der Wallonischen Region vom 30. September 2020 (Rechtssache Nr. 7555), der Ordonnanz der Gemeinsamen Gemeinschaftskommission vom 1. Oktober 2020 (Rechtssache Nr. 7559), des Dekrets der Flämischen Gemeinschaft vom 2. Oktober 2020 (Rechtssache Nr. 7560), von Artikel 2 des Gesetzes vom 9. Oktober 2020 (Rechtssachten Nrn. 7557 und 7558) und des Dekrets der Deutschsprachigen Gemeinschaft vom 12. Oktober 2020 (Rechtssache Nr. 7556) « zur Billigung 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, Gesundheitsinspektionsdienste und mobilen Teams im Rahmen einer Kontaktermittlung bei (vermutlich) mit dem Coronavirus COVID-19 infizierten Personen auf der Grundlage einer Datenbank bei Sciensano » (nachstehend: Zusammenarbeitsabkommen vom 25. August 2020).

Mit diesem Zusammenarbeitsabkommen vereinbaren die Föderalbehörde, die Flämische Gemeinschaft, die Wallonische Region, die Deutschsprachige Gemeinschaft und die Gemeinsame Gemeinschaftskommission die Schaffung von mehreren Datenbanken, um die manuelle Kontaktrückverfolgung und die digitale Kontaktrückverfolgung von Personen, die mit COVID-19 infiziert sind, von Personen, bei denen eine Infektion vermutet wird, und ihrer Kontakte zu organisieren, um die Ausbreitung des Virus zu begrenzen.

B.1.2. In ihrem Gutachten Nr. 67.719/VR vom 15. Juli 2020 zum Gesetzesvorentwurf, der zum angefochtenen Gesetz vom 9. Oktober 2020 geführt hat, hat die Gesetzgebungsabteilung

des Staatsrates den Entwurf des Zusammenarbeitsabkommens beschrieben. Diese Beschreibung ist auf den endgültigen Text des Zusammenarbeitsabkommens mithilfe einiger Anpassungen, die in eckigen Klammern angegeben sind, entsprechend anwendbar:

« 5.1. L'accord de coopération crée auprès de Sciensano quatre bases de données (Bases de données I, III, IV et V), à côté de la base de données existante, dont les modalités sont définies au regard de la lutte contre le COVID-19 (Base de données II). L'article 1er, § 1er, [6° à 10°], de l'accord de coopération décrit ces cinq bases de données.

- La Base de données I est la base de données centrale générale créée auprès de Sciensano pour le traitement et l'échange de données aux fins de traitement fixées dans l'accord de coopération. […]

- La Base de données II est la base de données existante auprès de Sciensano créée en exécution d'un accord de coopération [lire : une convention de collaboration] conclu avec l'Institut national d'assurance maladie-invalidité (ci-après : INAMI) […]. Les données […] doivent permettre aux institutions de recherche, dont Sciensano, d'effectuer des études scientifiques ou statistiques en rapport avec la propagation du coronavirus COVID-19 et de soutenir la politique de lutte contre le coronavirus par l'échange des données avec la Base de données I [article 1er, § 2, 3°].

- La Base de données III est la base de données [des instructions d'appel et des instructions] pour le personnel du centre de contact.

- La Base de données IV est la base de données contenant les coordonnées des collectivités.

- La Base de données V est le journal central des enregistrements qui permet de contrôler le fonctionnement de l'application numérique de traçage des contacts et qui, au sein de Sciensano, est séparée des Bases de données I et II. Une application numérique de traçage des contacts sur la base du DP3T se compose en effet d'une application mobile qui peut être, sur une base volontaire, installée et utilisée par l'utilisateur en local sur son appareil, et d'un journal central des enregistrements conservés dans la Base de données V [article 14, § 3, 1° et 2°, et § 5].

5.2. Le chapitre Ier de l'accord de coopération contient des dispositions générales. L'article 1er comporte un certain nombre de définitions (paragraphe 1er), mentionne les objectifs de l'accord de coopération (paragraphe 2), indique qu'il n'est pas porté préjudice à la réglementation des autorités compétentes en matière de suivi des contacts pour la détection des maladies contagieuses (paragraphe 3), requiert que les parties doivent prendre les mesures nécessaires à la mise en œuvre de l'accord de coopération et à l'harmonisation de leurs initiatives existantes avec cet accord (paragraphe 4), prévoit la possibilité d'accords de coopération d'exécution (paragraphe 5) et dispose que les prestataires des soins de santé et les personnes contactées sont relevées de leur secret professionnel (paragraphe 6). L'article 2 crée la Base de données I (paragraphe 1er), inscrit la Base de données II dans le cadre de cet accord de coopération (paragraphe 2), crée les Bases de données III et IV (paragraphe 3), désigne Sciensano comme responsable du traitement des Bases de données I et II (paragraphe 4) et

dispose que les entités fédérées [ou leurs agences] désigneront les responsables du traitement des Bases de données III et IV (paragraphe 5).

Le chapitre II contient l'article 3, qui règle les finalités du traitement concernant la mise à disposition des données à caractère personnel par la Base de données I (paragraphe 1er), ainsi que le traitement des données à caractère personnel [par les entités fédérées] ou les agences compétentes (paragraphe 2) et par les équipes mobiles et les inspections d'hygiène des communautés (paragraphe 3). Une interdiction générale de traitement des données à caractère personnel à d'autres fins est énoncée (paragraphe 4).

Le chapitre III contient l'article 4, qui définit les catégories de personnes dont les données à caractère personnel sont traitées dans le cadre de l'accord de coopération à l'examen. Ces catégories sont définies à l'article 1er, § 1er, [13° à 18°].

- Personnes de catégorie I : les personnes pour lesquelles le médecin a prescrit un test de dépistage du COVlD-19;

- Personnes de catégorie II : les personnes qui ont été soumises à un test de dépistage du COVID-19;

- Personnes de catégorie III : les personnes [pour lesquelles] le médecin [a une présomption sérieuse qu'elles sont] infectées, sans qu'un test de dépistage du COVID-19 ait été effectué ou prescrit, ou dont le test de dépistage du COVID-19 a révélé qu'elles n'étaient pas infectées;

- Personnes de catégorie IV : les personnes avec lesquelles soit (i) les Personnes de catégorie II dans la mesure où le test de dépistage du COVID-19 a révélé qu'elles sont infectées, soit (ii) les Personnes de catégorie III ont été en contact pendant une période de quatorze jours avant et après les premiers signes d'infection;

- Personnes de catégorie V : les médecins traitants des Personnes de catégories I, II et III;

- Personnes de catégorie VI : le médecin de référence ou – en l'absence d'un médecin de référence au sein de la collectivité concernée – le responsable administratif des collectivités avec lesquelles les Personnes des catégories I, II et III ont été en contact pendant une période de quatorze jours avant et après les premiers symptômes de l'infection.

Le chapitre IV détermine les catégories de données à caractère personnel qui sont traitées dans le cadre de l'accord de coopération. L'article 5 prescrit que le traitement des données doit être effectué conformément au RGPD et à la loi du 30 juillet 2018 ' relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel '. L'article 6 requiert que les déclarations obligatoires en vertu de la réglementation communautaire soient faites auprès de la Base de données I (paragraphe 1er) et définit les catégories de données à caractère personnel qui sont traitées dans cette base de données, respectivement, pour les Personnes de catégorie I, les Personnes de catégorie II, les Personnes de catégorie III et les Personnes de catégorie IV (paragraphes 2 à 5). Les paragraphes 6 et 7 définissent les données à caractère personnel supplémentaires à traiter pour certaines catégories de personnes et de clusters, qui sont collectées ou fournies par [les centres de contact,] les équipes mobiles ou les inspections d'hygiène compétentes. L'article 7 définit les catégories de données à caractère personnel qui sont traitées dans la Base de données III, à savoir les données à caractère

personnel qui sont communiquées par Sciensano à partir de la Base de données I aux centres de contact (paragraphe 1er), les données à caractère personnel pour la Base de données III en ce qui concerne les Personnes de catégorie II qui, après avoir effectué un test de dépistage du COVID-19, se sont avérées infectées, et les Personnes de catégorie III (paragraphe 2), les Personnes de catégorie IV (paragraphe 3) et les Personnes de catégorie VI (paragraphe 4). L'article 8 définit les catégories de données à caractère personnel qui sont traitées dans la Base de données IV en ce qui concerne les Personnes de catégorie V et de catégorie VI. L'article 9 définit les catégories de données à caractère personnel qui, après pseudonymisation, sont traitées dans la Base de données II en ce qui concerne les Personnes de catégorie I, de catégorie II et de catégorie III (paragraphe 1er) et les Personnes de catégorie IV (paragraphe 2).

Le chapitre V comporte l'article 10 qui règle l'accès aux données à caractère personnel par les centres de contact (paragraphe 1er) et par les équipes mobiles et les services d'inspection d'hygiène (paragraphe 2) ainsi que la transmission des données à caractère personnel, après pseudonymisation, de la Base de données I à la Base de données II (paragraphe 3).

Le chapitre VI concerne la compétence du Comité de sécurité de l'information. L'article 11 règle la délibération préalable, dans certains cas, au sein de ce comité (paragraphes 1er et 2) et la compétence de ce comité de préciser des données (paragraphe 3). Il est également prévu de régler certains aspects de l'accord de coopération dans un accord de coopération d'exécution (paragraphe 4). L'article 12 définit les modalités que le Comité de sécurité de l'information peut fixer (paragraphe 1er) et règle l'accès au Registre national et aux registres de la Banque-carrefour de la sécurité sociale (paragraphe 2), ainsi que la délibération préalable au sein du Comité de sécurité de l'information pour la communication [à la Base de données I] de données à caractère personnel provenant d'autres sources authentiques […] (paragraphe 3).

Le chapitre VII contient l'article 13, qui concerne les mesures de sécurité que Sciensano [et les entités fédérées compétentes ou leurs agences doivent prendre afin de garantir un niveau de sécurité adapté au risque.

Le chapitre VIII concerne les applications numériques de traçage des contacts. L'article 14 définit leur objectif (paragraphe 1er) et règle les limites du traitement des données à caractère personnel au moyen de ces applications (paragraphe 2), ainsi que les conditions minimales auxquelles ces applications doivent répondre (paragraphe 3). Celles-ci doivent respecter les principes énoncés [aux articles 5 et 25] du RGPD (paragraphe 4) et doivent se faire sur une base volontaire (paragraphe 5). Le délai de conservation des données relatives aux contacts est réglé (paragraphe 6), ainsi que les objectifs du traitement des données (paragraphe 7). Une analyse d'impact relative à la protection des données doit être établie et publiée (paragraphe 8). Il est également prévu de préciser certains aspects des applications numériques de traçage des contacts dans un accord de coopération d'exécution (paragraphe 9).

Le chapitre IX contient l'article 15, qui règle le délai de conservation maximal des données à caractère personnel pour les Bases de données I, III, IV et V (paragraphe 1er) et II (paragraphe 2).

Le chapitre X concerne la transparence et les droits des personnes concernées. L'article 16 énonce l'obligation pour Sciensano en tant que responsable du traitement de prendre des mesures appropriées en matière de communication des droits des personnes concernées (paragraphe 1er), créer et à assurer la maintenance d'un site internet (paragraphe 2), gérer et assurer la maintenance d'un système pour l'exercice des droits prévus dans le RGPD

(paragraphe 3) et conclure un accord avec les [entités fédérées] et leurs agences en ce qui concerne leurs responsabilités en matière d'exercice des droits des personnes concernées et la fourniture d'informations (paragraphe 4).

Le chapitre [XI] contient diverses dispositions finales. L'article 17 organise le règlement des litiges entre les parties par une juridiction de coopération. L'article 18 charge la Conférence interministérielle Santé publique de surveiller la mise en œuvre et le respect des dispositions de l'accord de coopération, […] de proposer des adaptations [et d'exercer une fonction de médiation]. L'article 19 règle l'entrée en vigueur rétroactive de l'accord de coopération (paragraphe 1er) et prévoit [que ses mesures prennent fin le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie de COVID-19 (paragraphe 2) ainsi que] la possibilité de sa résiliation par un nouvel accord de coopération (paragraphe [3]) » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, SS. 31-35).

B.1.3. Gemäß Artikel 1 § 2 hat das Zusammenarbeitsabkommen vom 25. August 2020 das dreifache Ziel, (1) einen Rahmen für die manuelle Kontaktermittlung und den Einsatz mobiler Teams zu schaffen, (2) einen Rahmen für die digitale Kontaktermittlung anhand einer digitalen Kontaktrückverfolgungsanwendung zu schaffen und (3) den Forschungseinrichtungen und Verwaltungen, einschließlich Sciensano, die Durchführung wissenschaftlicher oder statistischer Studien über die Bekämpfung der Ausbreitung des Coronavirus COVID-19 zu ermöglichen und/oder die in diesem Bereich geführte Politik zu unterstützen.

Aus den allgemeinen Erläuterungen des Zusammenarbeitsabkommens geht hervor, dass die digitale Kontaktrückverfolgung die manuelle Ermittlung ergänzen soll (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, S. 72).

Das Zusammenarbeitsabkommen zielt insbesondere darauf ab, mit COVID-19 infizierten Personen und potenziell infizierten Personen oder Personen, bei denen eine Infektion vermutet wird, Empfehlungen zu geben, um Infektionsketten zu unterbrechen. Aus Artikel 1 § 2 Nr. 1 Buchstabe *f)* des Zusammenarbeitsabkommens geht hervor, dass diese Empfehlungen für die betroffenen Personen nicht verpflichtend sind.

B.1.4. Vor dem Zusammenarbeitsabkommen vom 25. August 2020 wurde die Schaffung einer Datenbank, um die manuelle Kontaktrückverfolgung im Rahmen der Bekämpfung von COVID-19 zu ermöglichen, durch den königlichen Erlass Nr. 18 vom 4. Mai 2020 « zur Schaffung einer Datenbank bei Sciensano im Rahmen der Bekämpfung der Ausbreitung des Coronavirus COVID-19 » (nachstehend: königlicher Erlass Nr. 18 vom 4. Mai 2020) geregelt. Dieser Erlass mit einer Geltungsdauer, die ursprünglich bis zum 4. Juni 2020 festgelegt wurde

(Artikel 6), wurde durch Artikel 2 des königlichen Erlasses Nr. 25 vom 28. Mai 2020 « zur Abänderung des Königlichen Erlasses Nr. 18 vom 4. Mai 2020 zur Schaffung einer Datenbank bei Sciensano im Rahmen der Bekämpfung der Ausbreitung des Coronavirus COVID-19 » (nachstehend: königlicher Erlass Nr. 25 vom 28. Mai 2020) bis zum 30. Juni 2020 verlängert.

Am 14. Mai 2020 wurde ein Gesetzesvorschlag « zur Schaffung einer Datenbank bei Sciensano im Rahmen der Bekämpfung der Ausbreitung des Coronavirus COVID-19 » der Kammer mit dem gleichen Ziel vorgelegt (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1249/001). Ein zweiter Gesetzesvorschlag « über die Nutzung von digitalen Kontaktrückverfolgungsanwendungen als Präventionsmaßnahme gegen die Ausbreitung des Coronavirus COVID-19 in der Bevölkerung », der am Vortag eingereicht worden war, zielte seinerseits darauf ab, einen Rahmen für die digitale Kontaktrückverfolgung mithilfe von digitalen Anwendungen zu schaffen (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1251/001). Mit ihren Gutachten Nrn. 67.425/3-67.426/3-67.427/3 und 67.424/3 vom 26. Mai 2020 zu diesen zwei Gesetzesvorschlägen hat die Gesetzgebungsabteilung des Staatsrates die Notwendigkeit festgestellt, in Anbetracht des engen Zusammenhangs der von den geplanten Maßnahmen betroffenen föderalen Zuständigkeiten und Zuständigkeiten der Gemeinschaften ein Zusammenarbeitsabkommen zwischen der Föderalbehörde und den Gemeinschaften abzuschließen (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1249/006, SS. 6-9; *Parl. Dok.*, Kammer, 2019-2020, DOC 55-1251/003, SS. 5-8). Sie hat diese Schlussfolgerung in ihrem Gutachten Nr. 67.482/3 vom 3. Juni 2020 bekräftigt, das zu einem umfassenden Abänderungsantrag zu dem vorerwähnten ersten Gesetzesvorschlag, mit dem dieser ersetzt werden sollte, abgegeben wurde (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1249/009, SS. 5-7).

Am 25. Juni 2020 hat der Konzertierungsausschuss den Entwurf des Zusammenarbeitsabkommens, der zum Zusammenarbeitsabkommen vom 25. August 2020 geführt hat, angenommen.

Bis zur Beendigung der Gesetzesverfahren zur Billigung des Entwurfs des Zusammenarbeitsabkommens hat der königliche Erlass Nr. 44 vom 26. Juni 2020 « in Bezug auf die gemeinsame Verarbeitung von Daten durch Sciensano und die von den zuständigen Regionalbehörden oder von den zuständigen Agenturen bestimmten Kontaktzentren, Gesundheitsinspektionsdienste und mobilen Teams im Rahmen einer Kontaktermittlung bei

(vermutlich) mit dem Coronavirus COVID-19 infizierten Personen auf der Grundlage einer Datenbank bei Sciensano » (nachstehend: königlicher Erlass Nr. 44 vom 26. Juni 2020) den Inhalt des Entwurfs des Zusammenarbeitsabkommens im Wesentlichen übernommen. Dieser Erlass ist am 1. Juli 2020 in Kraft getreten. Nach seinem Artikel 17 sollte er am Tag des Inkrafttretens des Zusammenarbeitsabkommens und spätestens am 15. Oktober 2020 außer Kraft treten.

Der königliche Erlass Nr. 18 vom 4. Mai 2020, der königliche Erlass Nr. 25 vom 28. Mai 2020 und der königliche Erlass Nr. 44 vom 26. Juni 2020 wurden durch die Artikel 3 bis 5 des angefochtenen Gesetzes vom 9. Oktober 2020 zurückgenommen.

B.1.5. Gemäß seinem Artikel 19 § 1 Absatz 1 sind die Bestimmungen des Zusammenarbeitsabkommens vom 25. August 2020, die inhaltlich mit den Bestimmungen des königlichen Erlasses Nr. 18 vom 4. Mai 2020 übereinstimmen, rückwirkend zum Datum des Inkrafttretens dieses königlichen Erlasses am 4. Mai 2020 in Kraft getreten. Gemäß seinem Artikel 19 § 1 Absatz 2 sind Artikel 14 des Zusammenarbeitsabkommens vom 25. August 2020 und die Bestimmungen desselben Zusammenarbeitsabkommens über die digitalen Kontaktrückverfolgungsanwendungen rückwirkend zum 29. Juni 2020, « was die Bestimmungen betrifft, die inhaltlich mit dem Königlichen Erlass Nr. 44 vom 26. Juni 2020 […] übereinstimmen », in Kraft getreten.

Artikel 19 § 2 des Zusammenarbeitsabkommens vom 25. August 2020 sieht vor, dass seine Maßnahmen unbeschadet der Bestimmungen des Artikels 15 §§ 2 und 3 am Tag der Veröffentlichung des königlichen Erlasses zur Erklärung der Beendigung des Zustands der COVID-19-Epidemie aufhören, wirksam zu sein.

In Bezug auf das Interesse der klagenden Parteien

B.2.1. Der Ministerrat, die Wallonische Regierung, die Flämische Regierung, die Regierung der Deutschsprachigen Gemeinschaft und das Vereinigte Kollegium der Gemeinsamen Gemeinschaftskommission (nachstehend: die beklagten Behörden) machen geltend, dass die Nichtigkeitsklagen unzulässig seien, weil ein Interesse fehle.

B.2.2. Die Verfassung und das Sondergesetz vom 6. Januar 1989 über den Verfassungsgerichtshof erfordern, dass jede natürliche oder juristische Person, die eine Nichtigkeitsklage erhebt, ein Interesse nachweist. Das erforderliche Interesse liegt nur bei jenen Personen vor, deren Situation durch die angefochtenen Rechtshandlungen unmittelbar und ungünstig beeinflusst werden könnte.

B.2.3. Die zweite bis vierte klagende Partei in den Rechtssachen Nrn. 7555, 7556, 7558, 7559 und 7560 machen ihre Eigenschaft als natürliche Person zur Begründung ihres Interesses geltend.

Mit den angefochtenen Akten wird das Zusammenarbeitsabkommen vom 25. August 2020 gebilligt, das einen rechtlichen Rahmen für die manuelle und digitale Rückverfolgung der Kontakte von mit dem Coronavirus infizierten Personen schafft, um dessen Ausbreitung zu verhindern. Dieses Zusammenarbeitsabkommen sieht die Sammlung von zahlreichen personenbezogenen Daten, auch von sensiblen Daten bezüglich der Gesundheit insbesondere über Personen vor, die Kontakt zu einer positiv auf das Coronavirus getesteten Person oder zu einer Person, bei der eine Infektion vermutet wird, hatten.

Dieses Zusammenarbeitsabkommen, so wie es durch die angefochtenen Akte gebilligt wurde, beeinflusst also unmittelbar und ungünstig die Situation jeder natürlichen Person, sie sich auf belgischem Hoheitsgebiet befindet.

Ein Zusammenarbeitsabkommen, das eine Zustimmung des Gesetzgebers erfordert, entfaltet seine Folgen erst vollständig, nachdem es von sämtlichen betroffenen gesetzgebenden Versammlungen gebilligt wurde.

Die zweite bis vierte klagende Partei in den Rechtssachen Nrn. 7555, 7556, 7558, 7559 und 7560 weisen daher ein Interesse an der Beantragung der Nichtigerklärung sämtlicher Zustimmungsakte zum Zusammenarbeitsabkommen vom 25. August 2020 nach.

Das Interesse der ersten klagenden Partei in diesen Rechtssachen braucht nicht geprüft zu werden.

B.2.4. Die Klage in der Rechtssache Nr. 7557 bezieht sich auf Artikel 2 des Gesetzes vom 9. Oktober 2020, das auch der in der Rechtssache Nr. 7558 angefochtene Akt ist, und stützt sich auf einen ähnlichen Klagegrund wie den in dieser Rechtssache angeführten Klagegrund. Da die zweite bis vierte klagende Partei in der Rechtssache Nr. 7558 ein Interesse an der Nichtigerklärung von Artikel 2 des Gesetzes vom 9. Oktober 2020 nachweisen, ist es nicht erforderlich, das Interesse der klagenden Partei in der Rechtssache Nr. 7557 zu prüfen.

B.2.5. Die Einrede wird abgewiesen.

In Bezug auf die Zulässigkeit des einzigen Klagegrunds

B.3.1. Nach Ansicht der beklagten Behörden ist der einzige Klagegrund unzulässig, weil er in Wirklichkeit nur gegen das Zusammenarbeitsabkommen vom 25. August 2020 gerichtet sei.

B.3.2. Der Gerichtshof ist dafür zuständig, durch Entscheid über Klagen auf Nichtigerklärung von Gesetzen, Dekreten und Ordonnanzen zu befinden. Diese Zuständigkeit umfasst die Akte zur Billigung eines Zusammenarbeitsabkommens. Der Gerichtshof ist jedoch nicht dafür zuständig, ein Zusammenarbeitsabkommen für nichtig zu erklären.

Die klagenden Parteien können jedoch die Akte zur Akte zur Billigung eines Zusammenarbeitsabkommens nicht sachdienlich anfechten und der Gerichtshof kann sie nicht sachdienlich prüfen, ohne in ihre Kritik oder seine Prüfung den Inhalt der relevanten Bestimmungen des gebilligten Zusammenarbeitsabkommens einzubeziehen.

B.3.3. Insoweit er formell gegen die Akte zur Billigung des Zusammenarbeitsabkommens vom 25. August 2020 und inhaltlich gegen die Bestimmungen dieses Zusammenarbeitsabkommens gerichtet ist, ist der einzige Klagegrund zulässig.

B.4.1. Die beklagten Behörden führen an, dass der einzige Klagegrund unzulässig sei, insofern er aus einem Verstoß gegen die Artikel 10 und 11 der Verfassung abgeleitet sei, weil die klagenden Parteien nicht die zwei Personenkategorien identifizierten, die in den angefochtenen Akten diskriminierend behandelt würden.

B.4.2. Wenn ein Verstoß gegen den Grundsatz der Gleichheit und Nichtdiskriminierung in Verbindung mit einem anderen Grundrecht geltend gemacht wird, das in der Verfassung oder in einer Bestimmung internationalen Rechts gewährleistet ist oder sich aus einem allgemeinen Rechtsgrundsatz herleitet, muss die Personenkategorie, deren Grundrecht verletzt wird, mit der Personenkategorie verglichen werden, für die dieses Grundrecht gewährleistet wird.

B.4.3. Da die Artikel 10 und 11 der Verfassung in Verbindung mit mehreren Bestimmungen geltend gemacht werden, die das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten gewährleisten, wird die Einrede abgewiesen.

B.5.1. In der Rechtssache Nr. 7556 führen die beklagten Behörden an, dass der einzige Klagegrund unzulässig sei, insofern die klagenden Parteien nicht die Bestimmung des Dekrets der Deutschsprachigen Gemeinschaft vom 12. Oktober 2020 angeben würden, deren Nichtigerklärung sie beantragten.

In allen Rechtssachen führen die beklagten Behörden an, dass der einzige Klagegrund unzulässig sei, insofern er abgeleitet sei aus einem Verstoß gegen Artikel 7 der Charta der Grundrechte der Europäischen Union (nachstehend: Charta) und die Artikel 4 Nummer 7, 35 und 36 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 « zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) » (nachstehend: DSGVO). Ihrer Auffassung nach versäumen es die klagenden Parteien anzugeben, inwiefern diese Bestimmungen verletzt würden.

B.5.2. Artikel 6 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof bestimmt:

« Die Klageschrift gibt den Gegenstand der Klage an und enthält eine Darlegung des Sachverhalts und der Klagegründe ».

Um den Erfordernissen dieser Bestimmung zu entsprechen, müssen die in der Klageschrift vorgebrachten Klagegründe angeben, welche Vorschriften, deren Einhaltung der Gerichtshof gewährleistet, verletzt wären und welche Bestimmungen gegen diese Vorschriften verstoßen

würden, und darlegen, in welcher Hinsicht diese Vorschriften durch diese Bestimmungen verletzt würden. Diese Erfordernisse beruhen einerseits auf der Notwendigkeit, den Gerichtshof in die Lage zu versetzen, ab dem Zeitpunkt des Einreichens der Klageschrift die richtige Tragweite der Nichtigkeitsklage bestimmen zu können, und andererseits darauf, den anderen Verfahrensparteien die Möglichkeit zu geben, die Argumente der klagenden Parteien zu erwidern, wofür eine klare und unzweideutige Darlegung der Klagegründe unentbehrlich ist.

B.5.3. Aus der Klageschrift in der Rechtssache Nr. 7556 kann geschlossen werden, dass die klagenden Parteien ihre Beschwerdegründe nur gegen Artikel 1 des Dekrets der Deutschsprachigen Gemeinschaft vom 12. Oktober 2020 richten, insofern mit dieser Bestimmung das Zusammenarbeitsabkommen vom 25. August 2020 gebilligt wird. Der Gerichtshof prüft folglich die anderen Bestimmungen dieses Dekrets nicht.

B.5.4. Die klagenden Parteien führen an, dass das Zusammenarbeitsabkommen vom 25. August 2020, wie es durch die angefochtenen Akte gebilligt wurde, gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten verstoße, die in Artikel 22 der Verfassung, in Artikel 8 der Europäischen Menschenrechtskonvention und in Artikel 7 der Charta gewährleistet sind, die eine ähnliche Tragweite haben.

Der einzige Klagegrund ist demzufolge zulässig.

B.5.5. Artikel 4 Nummer 7 der DSGVO definiert den Verantwortlichen.

Wenn sie im ersten Teil des einzigen Klagegrunds die Schaffung der Datenbank I bei Sciensano unter anderem aus dem Grund beanstanden, dass diese Einrichtung nicht mit den manuellen Vorgängen zur Kontaktrückverfolgung beauftragt sei, legen die klagenden Parteien dar, inwiefern Artikel 4 Nummer 7 der DSGVO verletzt wird.

Der einzige Klagegrund ist demzufolge zulässig.

B.5.6. Wenn die klagenden Parteien im dritten Teil des einzigen Klagegrunds anmerken, dass die Genehmigungsbefugnis des Informationssicherheitsausschusses auf der Grundlage von Artikel 36 Absatz 5 der DSGVO nicht gerechtfertigt werden könne, da dieser Ausschuss nicht

als eine Aufsichtsbehörde angesehen werden könne, legen sie dar, inwiefern diese Bestimmung verletzt wird.

Die klagenden Parteien legen hingegen weder dar, inwiefern Artikel 36 Absatz 4 der DSGVO, der die Konsultation der Aufsichtsbehörde bei der Ausarbeitung eines Vorschlags einer Gesetzgebungsmaßnahme oder Regelungsmaßnahme betrifft, noch inwiefern Artikel 35 der DSGVO und Artikel 36 Absätze 1 bis 3 der DSGVO, die die vorherige Abschätzung der Folgen der Verarbeitungsvorgänge, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, und die vorherige Konsultation der Aufsichtsbehörde in diesem Rahmen betreffen, verletzt würden.

Insofern er aus einem Verstoß gegen die Artikel 35 und 36 Absätze 1 bis 4 der DSGVO abgeleitet ist, ist der einzige Klagegrund unzulässig.

B.5.7. Die Wiedergabe, auch die vollständige Wiedergabe von Stellungnahmen eines Beratungsgremiums erfüllt nicht die vorerwähnten Erfordernisse von Artikel 6 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof. Die im zweiten Teil des einzigen Klagegrunds dargelegten Beschwerdegründe, die die Notwendigkeit, je nach angestrebtem Zweck die Daten und die Datenbank voneinander zu unterscheiden, die Notwendigkeit der Sammlung von personenbezogenen Daten der Personen der Kategorie IV in der Datenbank I und die fehlende Klarheit bestimmter Konzepte betreffen, sind daher unzulässig.

Zur Hauptsache

B.6. Der einzige Klagegrund ist abgeleitet aus einem Verstoß gegen die Artikel 10, 11 und 22, an sich oder in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8 und 52 der Charta und mit den Artikeln 4 Nummer 7, 5 Absatz 1, 6, 9, 14 und 36 Absatz 5 der DSGVO.

Die klagenden Parteien machen im Wesentlichen geltend, dass mehrere Bestimmungen des Zusammenarbeitsabkommens vom 25. August 2020, wie sie durch die angefochtenen Akte

gebilligt wurde, gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten verstoßen.

B.7.1. Artikel 22 der Verfassung bestimmt:

« Jeder hat ein Recht auf Achtung vor seinem Privat- und Familienleben, außer in den Fällen und unter den Bedingungen, die durch Gesetz festgelegt sind.

Das Gesetz, das Dekret oder die in Artikel 134 erwähnte Regel gewährleistet den Schutz dieses Rechtes ».

B.7.2. Artikel 8 der Europäischen Menschenrechtskonvention bestimmt:

« (1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer ».

B.7.3. Der Verfassungsgeber hat eine möglichst weitgehende Übereinstimmung zwischen Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention angestrebt (*Parl. Dok.*, Kammer, 1992-1993, Nr. 997/5, S. 2).

Die Tragweite dieses Artikels 8 entspricht derjenigen der vorerwähnten Verfassungsbestimmung, sodass die durch die beiden Bestimmungen gebotenen Garantien ein untrennbares Ganzes bilden.

B.7.4. Das Recht auf Achtung des Privatlebens, so wie es durch die vorerwähnten Verfassungs- und Vertragsbestimmungen gewährleistet wird, bezweckt im Wesentlichen, die Personen gegen Einmischungen in ihr Privatleben zu schützen.

In dem Vorschlag, der der Annahme von Artikel 22 der Verfassung voraufging, wurde « der Schutz der Person, die Anerkennung ihrer Identität, die Bedeutung ihrer Entfaltung sowie derjenigen seiner Familie » hervorgehoben, sowie die Notwendigkeit, das Privat- und Familienleben vor « den Gefahren einer Einmischung, unter anderem als Folge der ständigen

Entwicklung der Informationstechniken, wenn Maßnahmen zur Ermittlung, Untersuchung und Kontrolle durch die Behörden und durch private Einrichtungen bei der Ausführung ihrer Funktionen oder Tätigkeiten durchgeführt werden » zu schützen (*Parl. Dok.*, Senat, Sondersitzungsperiode 1991-1992, Nr. 100-4/2°, S. 3). In dem Vorschlag wurde ebenso ausgeführt, dass der Gesetzgeber « das Recht auf Achtung des Privat- und Familienlebens auf keinerlei Weise aushöhlen darf, andernfalls verletzt er nicht nur eine Verfassungsbestimmung, sondern auch internationale Rechtsvorschriften » (ebenda).

Das Recht auf Achtung des Privatlebens hat eine weitreichende Tragweite und umfasst unter anderem den Schutz der personenbezogenen Daten und der persönlichen Information. Die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zeigt, dass u.a. folgende personenbezogene Daten und Informationen unter den Schutzbereich dieses Rechts fallen: der Name, die Adresse, die professionellen Aktivitäten, die persönlichen Beziehungen, digitale Fingerabdrücke, Kamerabilder, Fotos, Kommunikationsdaten, DNA-Daten, gerichtliche Daten (Verurteilung oder Verdacht), finanzielle Daten, Informationen über Eigentum und medizinische Daten (siehe insbesondere EuGHMR, 26. März 1987, *Leander gegen Schweden*, §§ 47-48; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, §§ 66-68; 17. Dezember 2009, *B.B. gegen Frankreich*, § 57; 10. Februar 2011, *Dimitrov-Kazakov gegen Bulgarien*, §§ 29-31; 18. Oktober 2011, *Khelili gegen Schweiz*, §§ 55-57; 9. Oktober 2012, *Alkaya gegen Türkei*, § 29; 18. April 2013, *M.K. gegen Frankreich*, § 26; 18. September 2014, *Brunet gegen Frankreich*, § 31; 13. Oktober 2020, *Frâncu gegen Rumänien*, § 51).

B.7.5. Das Recht auf Achtung des Privatlebens ist jedoch kein absolutes Recht. Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention schließen eine Einmischung der Behörden in die Ausübung dieses Rechts nicht aus, sofern eine solche durch eine ausreichend präzise gesetzliche Bestimmung vorgesehen ist, sie einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft entspricht und sie im Verhältnis zu dem damit angestrebten rechtmäßigen Ziel steht. Diese Bestimmungen beinhalten außerdem die positive Verpflichtung für die Behörden, Maßnahmen zu ergreifen, die eine tatsächliche Achtung des Privatlebens gewährleisten, selbst in der Sphäre der gegenseitigen Beziehungen zwischen Einzelpersonen (EuGHMR, 27. Oktober 1994, *Kroon und andere gegen Niederlande*, § 31; Große Kammer, 12. November 2013, *Söderman gegen Schweden*, § 78).

Der Schutz personenbezogener Daten und insbesondere medizinischer Daten ist von grundlegender Bedeutung für das Recht auf Achtung des Privatlebens einer Person und um ihr Vertrauen in das Gesundheitssystem zu bewahren (EuGHMR, 25. Februar 1997, *Z. gegen Finnland*, § 95). Wenn sie die Abwägung zwischen dem Interesse des Staates an der Verarbeitung personenbezogener Daten und das Interesse des Einzelnen am Schutz der Vertraulichkeit dieser Daten vornehmen, verfügen die nationalen Behörden über einen gewissen Beurteilungsspielraum (ebenda, § 99). In Anbetracht der grundlegenden Bedeutung des Schutzes personenbezogener Daten ist dieser Spielraum jedoch recht begrenzt (EuGHMR, 26. Januar 2017, *Surikov gegen Ukraine*, § 73). Damit eine Norm mit dem Recht auf Achtung des Privatlebens vereinbar ist, ist es erforderlich, dass ein faires Gleichgewicht zwischen allen betroffenen Rechten und Interessen hergestellt wird. Bei der Beurteilung dieses Gleichgewichts sind unter anderem die Bestimmungen des Übereinkommens des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (nachstehend: Übereinkommen Nr. 108) zu berücksichtigen (EuGHMR, 25. Februar 1997, *Z gegen Finnland*, § 95; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, § 103; 26. Januar 2017, *Surikov gegen Ukraine*, § 74).

Das Übereinkommen Nr. 108 beinhaltet u.a. die Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Verhältnismäßigkeit, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit und Rechenschaftspflicht.

Dasselbe Übereinkommen wird durch ein Änderungsprotokoll aktualisiert, das am 10. Oktober 2018 zur Unterzeichnung aufgelegt wurde.

Aus dem Übereinkommen Nr. 108 ergibt sich, dass das innerstaatliche Recht insbesondere gewährleisten muss, dass die personenbezogenen Daten unter Berücksichtigung der Zwecke, für die sie erhoben oder gespeichert werden, erheblich sind und nicht darüber hinausgehen, dass sie so aufbewahrt werden, dass der Betroffene nicht länger identifiziert werden kann, als es die Zwecke erfordern, und dass die gespeicherten Daten wirksam gegen unangemessene und missbräuchliche Nutzungen geschützt werden. Es hat auch vorgegeben, dass es von großer Bedeutung ist, dass im innerstaatlichen Recht klare und detaillierte Regeln zur Tragweite und Anwendung der betreffenden Maßnahmen sowie zu den Mindestgarantien vorgesehen sind, die unter anderem die Dauer, die Speicherung, die Nutzung, den Zugriff von Dritten, die Verfahren

zur Wahrung der Integrität und Vertraulichkeit von Daten und die Verfahren zu deren Vernichtung betreffen, sodass ausreichende Garantien gegen die Gefahr von Missbrauch und Willkür in jeder Phase der Datenverarbeitung existieren (EuGHMR, 26. Januar 2017, *Surikov gegen Ukraine*, § 74).

B.7.6. Innerhalb des Geltungsbereichs des Rechts der Europäischen Union gewährleisten Artikel 22 der Verfassung, Artikel 8 der Europäischen Menschenrechtskonvention und Artikel 7 der Charta analoge Grundrechte, während Artikel 8 der Charta einen spezifischen Rechtsschutz für personenbezogene Daten bietet.

B.7.7. Der Gerichtshof der Europäischen Union ist der Auffassung, dass sich die Achtung des Rechts auf Privatleben hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information erstreckt, die eine bestimmte oder bestimmbare natürliche Person betrifft (EuGH, Große Kammer, 9. November 2010, C-92/09 und C-93/09, *Volker und Markus Schecke und Eifert*, Randnr. 52; 16. Januar 2019, C-496/17, *Deutsche Post AG*, Randnr. 54).

B.7.8. Artikel 52 Absatz 1 der Charta bestimmt:

« Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen ».

B.7.9. Artikel 4 Nummern 1, 2, 5, 7 und 15 der DSGVO bestimmt:

« Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. ‘ personenbezogene Daten ’ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‘ betroffene Person ’) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

2. ‘ Verarbeitung ’ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

[…]

5. ‘ Pseudonymisierung ’ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

[…]

7. ‘ Verantwortlicher ’ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

[…]

15. ‘ Gesundheitsdaten ’ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen ».

Artikel 5 der DSGVO mit der Überschrift « Grundsätze für die Verarbeitung personenbezogener Daten » bestimmt:

« (1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (‘ Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz ’);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken (‘ Zweckbindung ’);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (‘ Datenminimierung ’);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (‘ Richtigkeit ’);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden (‘ Speicherbegrenzung ’);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (‘ Integrität und Vertraulichkeit ’);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (‘ Rechenschaftspflicht ’) ».

Artikel 6 der DSGVO mit der Überschrift « Rechtmäßigkeit der Verarbeitung » bestimmt:

« (1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche - um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist - unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,

d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann ».

Artikel 9 der DSGVO mit der Überschrift « Verarbeitung besonderer Kategorien personenbezogener Daten » bestimmt:

« (1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,

[…]

h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

i) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich […].

[…]

(3) Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

(4) Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist ».

Artikel 14 der DSGVO mit der Überschrift « Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden » bestimmt:

« (1) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) zusätzlich die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) die Kategorien personenbezogener Daten, die verarbeitet werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

c) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

f) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;

g) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und - zumindest in diesen Fällen - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Der Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2

a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,

b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,

c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

(4) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(5) Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit

a) die betroffene Person bereits über die Informationen verfügt,

b) die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien oder soweit die in Absatz 1 des vorliegenden Artikels genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich

macht oder ernsthaft beeinträchtigt In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit,

c) die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder

d) die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen ».

Artikel 24 der DSGVO mit der Überschrift « Verantwortung des für die Verarbeitung Verantwortlichen » bestimmt:

« (1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

(3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen ».

Artikel 26 der DSGVO mit der Überschrift « Gemeinsam für die Verarbeitung Verantwortliche » bestimmt:

« (1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend

widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen ».

Artikel 36 der DSGVO mit der Überschrift « Vorherige Konsultation » bestimmt in den Absätzen 1 und 5:

« (1) Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

[…]

(5) Ungeachtet des Absatzes 1 können Verantwortliche durch das Recht der Mitgliedstaaten verpflichtet werden, bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung zu Zwecken der sozialen Sicherheit und der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren und deren vorherige Genehmigung einzuholen ».

B.8. Die Beschwerdegründe der klagenden Parteien beziehen sich auf folgende Aspekte:

I. die in Artikel 2 des Zusammenarbeitsabkommens vom 25. August 2020 erwähnte Schaffung der Datenbank I bei Sciensano und die in Artikel 15 erwähnte Aufbewahrungsfrist der in der Datenbank II gespeicherten Daten (erster und zehnter Teil) (B.9-B.26);

II. die Notwendigkeit, bestimmte in den Artikeln 6 bis 9 erwähnte Datenkategorien zu sammeln (zweiter Teil) (B.27-B.34);

III. die in den Artikeln 11 und 12 erwähnte, dem Informationssicherheitsausschuss erteilte Ermächtigung, die Mitteilung von personenbezogenen Daten an Dritte zu genehmigen (dritter Teil) (B.35.1-B.40);

IV. die in Artikel 3 § 1 Nr. 2 Buchstabe B erwähnte, durch die Kontaktzentren den behandelnden Ärzten zur Verfügung gestellte Information (vierter Teil) (B.41-B.43);

V. den in Artikel 3 § 1 Nr. 4 erwähnten Zweck der wissenschaftlichen Forschung (fünfter Teil) (B.44-B.48);

VI. die in Artikel 14 erwähnten Verbindungen zwischen der Datenbank I und der Datenbank V und der Begriff der « Risikokontakte » (sechster und siebter Teil) (B.49-B.52.3);

VII. der in Artikel 3 erwähnte Begriff des « physischen Besuchs » (achter Teil) (B.53-B.55.4);

VIII. die Geheimhaltungspflicht der Mitarbeiter der Kontaktzentren (neunter Teil) (B.56-B.62).

I. In Bezug auf die Schaffung der Datenbank I bei Sciensano und die Aufbewahrungsfrist der in der Datenbank II gespeicherten Daten (erster und zehnter Teil)

B.9. Im ersten Teil des einzigen Klagegrunds machen die klagenden Parteien geltend, dass die Schaffung der Datenbank I bei Sciensano, die in Artikel 2 des Zusammenarbeitsabkommens vom 25. August 2020, wie es durch die angefochtenen Akte gebilligt wurde, vorgesehen ist, eine unverhältnismäßige Einmischung in das Recht auf Achtung des Privatlebens und in das Recht auf Schutz personenbezogener Daten zur Folge habe, da Sciensano nicht mit den manuellen Vorgängen zur Kontaktrückverfolgung beauftragt sei und andere Mittel existierten, um das angestrebte Ziel zu erreichen, zum Beispiel indem die Kontaktzentren gebeten würden, den für die wissenschaftliche Forschung zuständigen Akteuren selbst die notwendigen Daten zur Verfügung zu stellen. Die klagenden Parteien führen ebenfalls an, dass die angefochtene Bestimmung gegen die Grundsätze der Legalität und der Vorhersehbarkeit verstoße, da sie es nicht ermögliche zu verstehen, inwiefern die Schaffung einer zentralen Datenbank notwendig und verhältnismäßig sei.

Im zehnten Teil des einzigen Klagegrunds führen die klagenden Parteien an, dass Artikel 15 des Zusammenarbeitsabkommens nicht dem Legalitätsprinzip genüge, da die Aufbewahrungsfrist der pseudonymisierten Daten, die in der Datenbank II gespeichert würden, darin nicht präzisiert sei.

Der Gerichtshof prüft diese Beschwerdegründe, die sich insbesondere auf die Einhaltung des Legalitätsprinzips durch zusammenhängende Bestimmungen beziehen, zusammen.

B.10.1. Wie in B.7.4 erwähnt, schließt das Recht auf Achtung des Privatlebens den Schutz personenbezogener Daten und persönlicher Informationen ein, zu denen insbesondere Gesundheitsdaten gehören.

Insofern sie die Zentralisierung einer großen Anzahl an personenbezogenen Daten, einschließlich sensibler Daten in Bezug auf die Gesundheit, vorsieht, hat die angefochtene Bestimmung eine Einmischung in das Recht auf Achtung des Privatlebens und in das Recht auf Schutz personenbezogener Daten zur Folge, wie sie durch die in B.7 bis B.8 zitierten Bestimmungen gewährleistet werden.

B.10.2. Wie in B.7.5 darüber erwähnt, ist eine solche Einmischung nur zulässig, wenn sie durch eine ausreichend präzise gesetzliche Bestimmung vorgesehen ist, wenn sie einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft entspricht und wenn sie im Verhältnis zu dem damit angestrebten rechtmäßigen Ziel steht.

Da die in die Datenbank I übernommenen Daten insbesondere Daten bezüglich der Gesundheit im Sinne von Artikel 4 Nummer 15 der DSGVO darstellen und die angefochtene Bestimmung die Durchführung von mehreren Verarbeitungen dieser Daten im Sinne von Artikel 4 Nummer 2 der DSGVO voraussetzt, muss die Einmischung ebenfalls den in Artikel 9 der DSGVO festgelegten Bedingungen genügen.

Artikel 9 Absatz 1 der DSGVO untersagt grundsätzlich die Verarbeitung von sensiblen personenbezogenen Daten wie Daten über die Gesundheit. Artikel 9 Absatz 2 Buchstabe h) der DSGVO erlaubt jedoch eine solche Verarbeitung, wenn sie « für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs » erforderlich ist und einer beruflichen Geheimhaltungspflicht unterliegt. Artikel 9 Absatz 2 Buchstabe i) der DSGVO sieht vor, dass die Verarbeitung solcher Daten ebenfalls erlaubt ist,

wenn sie « aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht » erforderlich ist.

B.11.1. Insoweit sie einen Verstoß gegen das Legalitätsprinzip und den Grundsatz der Vorhersehbarkeit aus der nicht notwendigen und unverhältnismäßigen Beschaffenheit der angefochtenen Bestimmung ableiten, verwechseln die klagenden Parteien die verschiedenen Stufen der Prüfung, die der Gerichtshof in Bezug auf die Achtung des Rechts auf Privatleben und des Rechts auf Schutz personenbezogener Daten vornehmen muss.

B.11.2. Artikel 22 der Verfassung behält dem zuständigen Gesetzgeber die Befugnis vor, festzulegen, in welchen Fällen und unter welchen Bedingungen das Recht auf Achtung des Privatlebens beeinträchtigt werden kann. Somit garantiert er jedem Bürger, dass eine Einmischung in die Ausübung dieses Rechts nur aufgrund von Regeln erfolgen darf, die durch eine demokratisch gewählte beratende Versammlung angenommen wurden.

Eine Ermächtigung einer anderen Gewalt steht jedoch nicht im Widerspruch zum Legalitätsprinzip, sofern die Ermächtigung ausreichend präzise beschrieben ist und sich auf die Ausführung von Maßnahmen bezieht, deren wesentliche Elemente vorher durch den Gesetzgeber festgelegt wurden.

Folglich müssen die wesentlichen Elemente der Verarbeitungen personenbezogener Daten im Gesetz selbst festgelegt sein. Diesbezüglich sind unabhängig vom betroffenen Gebiet die folgenden Elemente grundsätzlich wesentlich: (1.) die Kategorien der verarbeiteten Daten, (2.) die betroffenen Personenkategorien, (3.) der mit der Verarbeitung verfolgte Zweck, (4.) die Personenkategorien, die Zugriff auf die verarbeiteten Daten haben, und (5.) die maximale Dauer der Aufbewahrung der Daten (siehe in diesem Sinne das Gutachten der Generalversammlung der Gesetzgebungsabteilung des Staatsrates Nr. 68.936/AG vom 7. April 2021 zu einem Vorentwurf des Gesetzes « über verwaltungspolizeiliche Maßnahmen in einer epidemischen Notsituation », *Parl. Dok.*, Kammer, 2020-2021, DOC 55-1951/001, S. 119).

B.11.3. Neben dem formalen Erfordernis der Legalität wird durch Artikel 22 der Verfassung in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention und mit den Artikeln 7, 8 und 52 der Charta ebenfalls die Verpflichtung auferlegt, dass die Einmischung in die Ausübung des Rechts auf Achtung des Privatlebens und des Rechts auf den Schutz personenbezogener Daten deutlich und ausreichend präzise formuliert wird, damit es möglich ist, die Fälle vorherzusehen, in denen der Gesetzgeber eine solche Einmischung erlaubt.

Auf dem Gebiet des Datenschutzes bedeutet dieses Erfordernis der Vorhersehbarkeit, dass ausreichend präzise vorgesehen werden muss, unter welchen Umständen Verarbeitungen von personenbezogenen Daten erlaubt sind (EuGHMR, Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, § 57; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, § 99). In diesem Zusammenhang hat der Europäische Gerichtshof für Menschenrechte betont, dass es mehrere entscheidende Phasen gibt, in deren Verlauf sich Fragen zum Datenschutz im Hinblick auf Artikel 8 der Europäischen Menschenrechtskonvention stellen können, insbesondere bei der Erhebung, der Speicherung, der Nutzung und der Weitergabe von Daten (EuGHMR, 24. Januar 2019, *Catt. gegen Vereinigtes Königreich*, § 95).

Jeder muss somit eine ausreichend klare Vorstellung von den verarbeiteten Daten, den von einer bestimmten Datenverarbeitung betroffenen Personen und den Bedingungen und Zwecken dieser Verarbeitung haben können.

B.11.4. Somit prüft der Gerichtshof zunächst, ob jeder, dessen personenbezogene Daten in der Datenbank I und gegebenenfalls in den anderen von ihr gespeisten Datenbanken gesammelt und gespeichert werden, in Anbetracht der verschiedenen in der angefochtenen Bestimmung und den mit ihr verbundenen Bestimmungen enthaltenen Elemente in ausreichend präziser Weise wissen kann, unter welchen Bedingungen die Verarbeitung seiner Daten erfolgt.

1. Die Legalität und die Vorhersehbarkeit der Einmischung

B.12. Artikel 2 des Zusammenarbeitsabkommens vom 25. August 2020 bestimmt:

« § 1. Um die in Artikel 1 § 2 erwähnten Ziele zu erreichen, wird bei Sciensano eine Datenbank I eingerichtet, die die in Artikel 6 beschriebenen Datenkategorien enthält. Diese Daten werden zu den in Artikel 3 bestimmten Zwecken für eine Dauer verarbeitet, die in Artikel 15 festgelegt ist. Diese Daten werden von den dazu ermächtigten Personen oder den auf Anweisung der dazu ermächtigten Personen handelnden Personen der Krankenhäuser und der Labore sowie von den Ärzten und den Mitarbeitern der Kontaktzentren, der Gesundheitsinspektionsdienste und der mobilen Teams mitgeteilt.

§ 2. Die Datenbank I wird unbeschadet der bereits bestehenden Datenbank II eingerichtet.

Um das in Artikel 1 § 2 Nr. 1 Buchstabe *h)* und Nr. 3 erwähnte Ziel zu erreichen, werden die Daten der Datenbank I vor Aufnahme in die Datenbank II gemäß den Bestimmungen der Artikel 9 und 10 pseudonymisiert.

§ 3. Um die in Artikel 1 § 2 Nr. 1 Buchstabe *b)*, *e)*, *f)* und *g)* erwähnten Ziele zu erreichen, werden neben der Datenbank I folgende zeitweilige Datenbanken eingerichtet, zwischen denen die in Artikel 6 bestimmten Datenkategorien ausgetauscht werden, allerdings ausschließlich für die in Artikel 3 bestimmten Verarbeitungszwecke und gemäß den Bestimmungen von Artikel 10 und für die in Artikel 15 festgelegte Dauer:

1° Datenbank III,

2° Datenbank IV.

§ 4. Sciensano ist der für die Verarbeitung der Datenbanken I und II Verantwortliche.

§ 5. Die zuständigen föderierten Teilgebiete oder die von den zuständigen Behörden bestimmten Agenturen handeln jeweils in ihrem Zuständigkeitsbereich als für die Verarbeitung der Datenbanken III und IV Verantwortliche in Bezug auf die personenbezogenen Daten, die von den durch die zuständigen föderierten Teilgebiete oder Agenturen bestimmten Kontaktzentren erfasst und verwendet werden, und ergreifen geeignete Maßnahmen, damit die in Artikel 4 erwähnten Personen die in den Artikeln 13 und 14 der Datenschutz-Grundverordnung erwähnten Informationen und die in den Artikeln 15 bis 22 und Artikel 34 der Datenschutz-Grundverordnung erwähnten Mitteilungen im Zusammenhang mit den in Artikel 3 § 2 erwähnten Verarbeitungszwecken erhalten. Diese Informationenmüssen in knapper, transparenter, verständlicher und leicht zugänglicher Form und in klarer und einfacher Sprache bereitgestellt werden ».

B.13.1. Nach Artikel 1 § 1 Nr. 6 des Zusammenarbeitsabkommens vom 25. August 2020 ist die Datenbank I die « aufgrund des vorliegenden Zusammenarbeitsabkommens einzurichtende Sciensano-Datenbank für die Verarbeitung und den Austausch von Daten zu den in Artikel 3 bestimmten Verarbeitungszwecken ». Sciensano ist als Verantwortlicher dieser Datenbank benannt (Artikel 2 § 4 des Zusammenarbeitsabkommens vom 25. August 2020). Das ist die mit Rechtspersönlichkeit ausgestattete öffentliche Einrichtung, die insbesondere die gesetzlichen Aufträge hat, Stellungnahmen für die Gesundheitsbehörden zu erstellen, personenbezogene Daten bezüglich der Volksgesundheit oder im Zusammenhang mit der

Gesundheit zu verarbeiten und wissenschaftliche Analysen auf der Grundlage der verarbeiteten Informationen durchzuführen, um die Gesundheitspolitik zu unterstützen (Artikel 3 und 4 § 1 Nr. 1 und § 4 des Gesetzes vom 25. Februar 2018 « zur Schaffung von Sciensano »). Seit dem 17. Juni 2021 sieht Artikel 4/1 des Gesetzes vom 25. Februar 2018, eingefügt durch Artikel 63 des Gesetzes vom 13. Juni 2021 « zur Festlegung von Maßnahmen zur Bewältigung der COVID-19-Pandemie und anderer dringender Maßnahmen im Bereich der Gesundheitspflege », vor, dass « im Rahmen der Bewältigung von Krisen, die die Volksgesundheit betreffen, […] Sciensano den Auftrag [hat], die damit verbundenen wissenschaftlichen Aspekte zu koordinieren und zu implementieren, die Risiken anhand von spezifischen Analysen der gesammelten Daten zu überwachen und zu evaluieren, gegenüber den verschiedenen Gesundheitsbehörden des Landes Stellungnahmen und Empfehlungen abzugeben und die Kommunikation für die Behörden, die Gesundheitsdienstleister und die Öffentlichkeit zu organisieren ». Mit dieser Bestimmung sollen die gesetzlichen Aufträge von Sciensano klar dargestellt und die Autorität und die Rolle dieser Einrichtung im Rahmen der Bewältigung von Gesundheitskrisen gestärkt werden (*Parl. Dok.*, Kammer, 2020-2021, DOC 55-1929/001, S. 60).

Aus dem verfügenden Teil des Zusammenarbeitsabkommens und den allgemeinen Erläuterungen geht hervor, dass die Datenbank I eine zentrale Datenbank bei Sciensano ist, um die personenbezogenen Daten zu sammeln, die einerseits von den Ärzten, den Laboren und den Krankenhäusern und andererseits vom Personal der Kontaktzentren und den mobilen Teams übermittelt werden (Artikel 2 § 1 dritter Satz des Zusammenarbeitsabkommens vom 25. August 2020; *Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, SS. 65 und 73). Das « Kontaktzentrum » ist die « von den zuständigen föderierten Teilgebieten oder den zuständigen Agenturen bestimmte Instanz, die mit der betreffenden Person im Rahmen der in Artikel 3 § 2 bestimmten Zwecke auf jedem möglichen Kommunikationsweg, einschließlich per Telefon, E-Mail oder durch einen physischen Besuch, in Kontakt tritt und anschließend die gesammelten Daten mit der Datenbank I teilt » (Artikel 1 § 1 Nr. 4). Die « mobilen Teams » sind die « Mitarbeiter des von den Gesundheitsinspektionsdiensten organisierten COVID–Unterstützungsteams (Outbreak Support Team), die im Falle eines Clusters Maßnahmen vor Ort ergreifen » (Artikel 1 § 1 Nr. 12). Ein « Cluster » ist die « Bündelung von Einzelpersonen in Personengemeinschaften, die mit dem Coronavirus COVID–19 infiziert oder vermutlich infiziert sind » (Artikel 1 § 1 Nr. 2). Eine « Personengemeinschaft » ist die « Gemeinschaft von Personen, für die die zuständigen Gesundheitsinspektionsdienste der Ansicht sind, dass ein

erhöhtes Risiko der Verbreitung des Coronavirus COVID–19 besteht » (Artikel 1 § 1 Nr. 3), zum Beispiel: ein Krankenhaus, eine Schule, ein Asylzentrum, ein Gefängnis, ein Alten- und Pflegeheim, eine Arbeitsstätte, eine Einrichtung für Personen mit Behinderung, eine Kindertagesstätte, ein Rehabilitationszentrum oder eine Kaserne (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, S. 76).

B.13.2. Die Datenbank I wird neben einer anderen Datenbank, die bereits bei Sciensano besteht (die Datenbank II) geschaffen. Die personenbezogenen Daten der Datenbank I werden nach Pseudonymisierung in der Datenbank II gespeichert, um sie zu wissenschaftlichen Forschungszwecken zu nutzen (Artikel 2 § 2). In den allgemeinen Erläuterungen des Zusammenarbeitsabkommens ist erwähnt, dass die Plattform « e-Health » für diese Pseudonymisierung verantwortlich ist, die erfolgt, nachdem die Daten in der Datenbank I gespeichert wurden und bevor sie mit der Datenbank II geteilt werden (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, SS. 69-74, insbesondere S. 71).

B.13.3. Durch das Zusammenarbeitsabkommen werden außerdem drei weitere Datenbanken geschaffen: eine gemeinsame Datenbank der Kontaktzentren, die Aufträge und Anrufaufträge für die Mitarbeiter der Kontaktzentren enthält (die Datenbank III), eine Datenbank mit den Kontaktdaten von Personengemeinschaften (die Datenbank IV) (Artikel 1 § 1 Nrn. 8 und 9 und Artikel 2 § 3) und die zentrale Logliste der digitalen Kontaktrückverfolgungsanwendung (die Datenbank V) (Artikel 1 § 1 Nr. 10 und Artikel 14 § 3 Nr. 2).

Die Datenbanken III und IV « tauschen untereinander und mit der Datenbank I im Rahmen der Kontaktermittlung Daten aus » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, S. 75; siehe Artikel 2 § 3). Die zuständigen föderierten Teilgebiete oder ihre Agenturen sind als Verantwortliche für die Datenbanken III und IV benannt (Artikel 2 § 5). Es handelt sich laut den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen um die Flämische Agentur « Zorg en Gezondheid », um die wallonische Agentur für Lebensqualität, um das Ministerium der Deutschsprachigen Gemeinschaft und die Gemeinsamen Gemeinschaftskommission (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, S. 74).

Sciensano ist der Verantwortliche für die Datenbank V (Artikel 14 § 3 Nr. 3), die bei Sciensano von den Datenbanken I und II getrennt ist (Artikel 1 § 1 Nr. 10).

B.13.4. Daraus ergibt sich, dass die Datenbank I die Quelle der personenbezogenen Daten darstellt, die an die für die wissenschaftliche Forschung genutzte Datenbank II übertragen werden. Sie stellt überdies die Quelle und den Empfänger der personenbezogenen Daten dar, die in der Datenbank III und in der Datenbank IV gesammelt werden. Aus dem vorerwähnten Artikel 1 § 1 Nr. 4 des Zusammenarbeitsabkommens und seiner allgemeinen Erläuterungen geht nämlich hervor, dass die Datenbank I insbesondere die von den Kontaktzentren bei den infizierten Personen und bei den vermutlich infizierten Personen erhobenen Informationen über die Personen, mit denen diese Kontakt hatten, und die von den mobilen Teams bei den Personengemeinschaften erhobenen Informationen umfasst:

« Afin de rendre le suivi manuel des contacts aussi efficace que possible, la Base de données I doit intervenir en tant que base de données centrale dans la lutte contre la propagation du coronavirus COVID-19. Sciensano, en tant que responsable du traitement, gère la Base de données I qui contient des données à caractère personnel fournies par les prestataires de soins et les établissements de soins. Toutefois, aux fins énoncées dans le présent accord de coopération, il sera également nécessaire que le personnel des centres de contact (y compris les enquêteurs de terrain) et les équipes mobiles partagent avec la Base de données I les données qu'ils ont recueillies. L'objectif est d'organiser un suivi manuel de contacts qui soit aussi efficace et complet que possible » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, S. 73).

« Les données collectées par les équipes mobiles peuvent en outre être transférées à Sciensano pour être stockées dans la Base de données I en vue de leur traitement et de leur communication ultérieur(e)s, mais uniquement pour les finalités de traitement fixées dans le présent accord de coopération » (ebenda, S. 89).

B.13.5. Hingegen ist die Datenbank I nicht mit der Datenbank V verbunden.

a) Die Zwecke der Verarbeitung

B.14.1. In Artikel 3 des Zusammenarbeitsabkommens vom 25. August 2020 sind die Zwecke der Verarbeitung der in der Datenbank I gesammelten personenbezogenen Daten « und des späteren Austauschs [dieser] Daten mit den Datenbanken II, III und IV » aufgezählt (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, S. 76).

B.14.2. Wie die Datenschutzbehörde in ihrer Stellungnahme Nr. 64/2020 vom 20. Juli 2020 zu dem Entwurf des Zusammenarbeitsabkommens, der zu dem

Zusammenarbeitsabkommen vom 25. August 2020 geführt hat, angemerkt hat, können diese Zwecke in drei Kategorien zusammengefasst werden (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/002, SS. 11-12).

Der erste Zweck besteht darin, es den Kontaktzentren zu ermöglichen, die manuelle Rückverfolgung der (vermutlich) infizierten Personen und ihrer Kontakte vorzunehmen (nachstehend: Zweck der manuellen Kontaktrückverfolgung). Zu diesem Zweck erhalten die Kontaktzentren über einen Datenaustausch zwischen der Datenbank I und der Datenbank III die Kategorien der personenbezogenen Daten über die Personen der Kategorie II, « insofern der COVID-19-Coronavirustest ergeben hat, dass sie infiziert sind » (nachstehend: positiv getestete Personen der Kategorie II), und über die vermutlich infizierten Personen (Personen der Kategorie III), um ihnen eventuelle Empfehlungen zu geben, aber vor allem um sie um Informationen über Personen, zu denen sie Kontakt hatten, zu bitten (Artikel 3 § 1 Nr. 1 in Verbindung mit Artikel 1 § 1 Nrn. 14 und 15 ; siehe auch Artikel 3 § 2 Nr. 1 und Artikel 10 § 1). Diese Informationen müssen es anschließend den Kontaktzentren ermöglichen, mit den Personen, mit denen die positiv getesteten Personen und die vermutlich infizierten Personen während eines Zeitraums von vierzehn Tagen vor und nach den ersten Anzeichen einer Infektion in Kontakt waren (Personen der Kategorie IV), in Kontakt zu treten, um ihnen Empfehlungen hinsichtlich Hygiene und Prävention zu geben, ihnen eine Quarantäne vorzuschlagen oder sie aufzufordern, sich testen zu lassen (Artikel 3 § 1 Nr. 2 A in Verbindung mit Artikel 1 § 1 Nr. 16; siehe auch Artikel 3 § 2 Nr. 2 A). Diese Informationen müssen es den Kontaktzentren auch ermöglichen, mit dem Referenzarzt oder dem Verwaltungsverantwortlichen der Personengemeinschaften, mit denen diese positiv getesteten und vermutlich infizierten Personen während eines Zeitraums von vierzehn Tagen vor und vierzehn Tagen nach den ersten Symptomen der Infektion mit dem Coronavirus COVID-19 Kontakt hatten (Personen der Kategorie VI), in Kontakt zu treten, um sie über die (vermutete) Infektion der vorerwähnten Personen zu informieren (Artikel 3 § 1 Nr. 2 B in Verbindung mit Artikel 1 § 1 Nr. 18; siehe auch Artikel 3 § 2 Nr. 2 B und Artikel 10 § 1).

Der zweite Zweck besteht darin, es den mobilen Teams und den Gesundheitsinspektionsdienste der föderierten Teilgebiete zu ermöglichen, Initiativen zur Vermeidung der Ausbreitung der schädlichen Auswirkungen des Coronavirus COVID-19 im Rahmen der Erfüllung ihrer verordnungsrechtlichen Aufträge zu ergreifen (nachstehend: Zweck der Prävention). Zu diesem Zweck haben die Teams und Dienste, die im flämischen

Dekret vom 21. November 2003 « über die präventive Gesundheitspolitik », im Dekret der Deutschsprachigen Gemeinschaft vom 1. Juni 2004 « zur Gesundheitsförderung und zur medizinischen Prävention » und in seinen Ausführungserlassen, in der Ordonnanz der Ordonnanz der Region Brüssel-Hauptstadt vom 19. Juli 2007 « über die präventive Gesundheitspolitik » im Dekret der Wallonischen Region vom 2. Mai 2019 « zur Abänderung des Wallonischen Gesetzbuches für soziale Aktion und Gesundheit hinsichtlich Prävention und Gesundheitsförderung », im Erlass des Vereinigten Kollegiums der Gemeinsamen Gemeinschaftskommission vom 23. April 2009 « über die Prophylaxe bei übertragbaren Krankheiten » und im Erlass der Flämischen Regierung vom 19. Juni 2009 « über die Initiativen zur Bekämpfung der Ausbreitung von schädlichen Auswirkungen durch biotische Faktoren » erwähnt sind, Zugriff auf die in der Datenbank I über Personen der Kategorien I bis IV gesammelten personenbezogenen Daten (Artikel 3 § 1 Nr. 3, Artikel 3 § 3 und Artikel 10 § 2).

Der dritte Zweck besteht darin, es den Forschungseinrichtungen, darunter Sciensano, zu ermöglichen, wissenschaftliche oder statistische Studien über die Bekämpfung der Ausbreitung von COVID-19 durchzuführen und/oder die Politik in diesem Bereich zu unterstützen (nachstehend: Zweck der wissenschaftlichen Forschung). Zu diesem Zweck werden die in der Datenbank I enthaltenen personenbezogenen Daten über Personen der Kategorien I bis V der Datenbank II in pseudonymisierter Form, sodann den Forschungseinrichtungen, darunter Sciensano, in anonymisierter oder zumindest in pseudonymisierter Form zur Verfügung gestellt (Artikel 3 § 1 Nr. 4 ; siehe auch Artikel 1 § 2 Nr. 1 Buchstabe *h)*, Artikel 1 § 2 Nr. 3 und Artikel 10 § 3 erster Satz).

B.14.3. In Artikel 3 § 4 heißt es, dass die im Rahmen des Zusammenarbeitsabkommens erhobenen Daten nicht zu anderen Zwecken verwendet werden dürfen, « insbesondere nicht - aber nicht ausschließlich - zu polizeilichen, kommerziellen, steuerrechtlichen, strafrechtlichen oder staatssicherheitlichen Zwecken ».

b) Die Kategorien der erhobenen personenbezogenen Daten und die Kategorien der betroffenen Personen

B.15.1. Artikel 6 §§ 2 bis 7 des Zusammenarbeitsabkommens vom 25. August 2020 bestimmt die Kategorien der in der Datenbank I enthaltenen personenbezogenen Daten für jede Kategorie der betroffenen Personen.

B.15.2. Für die Personen, die eine Verschreibung haben (Personen der Kategorie I) enthält die Datenbank I die folgenden Kategorien von personenbezogenen Daten: « 1° ENSS; 2° Namen und Vornamen; 3° Geschlecht; 4° Geburtsdatum und gegebenenfalls Sterbedatum; 5° Adresse; 6° Kontaktangaben, einschließlich Telefonnummer und E-Mail-Adresse der betreffenden Person und der im Notfall zu kontaktierenden Person oder des gesetzlichen Vertreters, und Angabe des Verhältnisses dieser Personen mit der betreffenden Person (Elternteil, Vormund, Allgemeinmediziner, ...); 7° Datum des Auftretens der Symptome; […]; 9° Angaben zum verschriebenen COVID–19-Coronavirustest, einschließlich Datum und Art des verschriebenen COVID–19-Coronavirustests; 10° Angabe der Ausübung oder Nicht-Ausübung des Berufs eines Gesundheitsdienstleisters; 11° Krankenhausabteilung, Identifikationsnummer und Angaben zum Standort des Krankenhauses, falls die betreffende Person im Krankenhaus behandelt wird; 12° gegebenenfalls Ergebnis des CT-Scans, wenn die betreffende Person im Krankenhaus behandelt wird; 13° Personengemeinschaft, der die betreffende Person gegebenenfalls angehört oder mit der sie in Kontakt gekommen ist » (Artikel 6 § 2 Absatz 1). Name und Vorname, Geburtsdatum, Geschlecht und Adresse stammen aus dem Nationalregister oder den Registern der Zentralen Datenbank der sozialen Sicherheit (Artikel 6 § 2 Absatz 2).

B.15.3. Für die getesteten Personen (Personen der Kategorie II) enthält die Datenbank I neben den in B.15.2 genannten Daten « 2° Datum, Ergebnis, Testnummer und Art des COVID–19-Coronavirustests; 3° LIKIV-Nummer des Labors, das den COVID–19-Coronavirustest durchgeführt hat; 4° im Falle eines Testergebnisses, auf dessen Grundlage keine Infektion festgestellt werden konnte, mögliche Entscheidung eines Arztes, sich darüber hinwegzusetzen; 5° im Falle eines Testergebnisses, auf dessen Grundlage keine Infektion festgestellt werden konnte, LIKIV-Nummer des Arztes, der die Entscheidung, sich über das Testergebnis hinwegzusetzen, getroffen hat » (Artikel 6 § 3 Absatz 1).

Diese Daten werden von « den dazu ermächtigten Personen oder den auf Anweisung der dazu ermächtigten Personen handelnden Personen des Labors, des Krankenhauses oder einer anderen Pflegeanstalt oder eines anderen Gesundheitsdienstleisters, die den COVID–

19-Corona Virustest durchgeführt haben » mitgeteilt, außer der möglichen von einem Arzt getroffenen Entscheidung, sich im Falle eines negativen Testergebnisses darüber hinwegzusetzen, und der LIKIV-Nummer dieses Arztes, die von dem betreffenden Arzt mitgeteilt werden (Artikel 6 § 3 Absatz 2).

B.15.4. Für die vermutlich infizierten Personen (Personen der Kategorie III) enthält die Datenbank I neben den in den Nrn. 1 bis 7, 10 und 13 erwähnten Daten, die in B.15.2 genannt wurden, « 7° voraussichtliche Diagnose der Infektion […]; 8° LIKIV-Nummer des Arztes, der den ernsthaften Verdacht formuliert […]; 12° Daten, die das Kontaktzentrum benötigt, um einen sachdienlichen Kontakt mit der betreffenden Person herzustellen, einschließlich Postleitzahl und Sprache » (Artikel 6 § 4 Absatz 1). Name und Vorname, Geburtsdatum, Geschlecht und Adresse stammen aus dem Nationalregister oder den Registern der Zentralen Datenbank der sozialen Sicherheit (Artikel 6 § 4 Absatz 2 zweiter Satz).

Diese Daten werden von dem Arzt, der den Verdacht einer Infektion hat, mitgeteilt (Artikel 6 § 4 Absatz 2 erster Satz).

B.15.5. Für die Personen, die Kontakt zu einer positiv getesteten oder zu einer vermutlich infizierten Person gehabt haben (Personen der Kategorie IV) und gegebenenfalls für die positiv getesteten Personen der Kategorie II und für die vermutlich infizierten Personen (Personen der Kategorie III) enthält die Datenbank I: « 1° ENSS; 2° Namen und Vornamen; 3° Geschlecht; 4° Geburtsdatum und gegebenenfalls Sterbedatum; 5° Adresse; 6° Kontaktangaben, einschließlich Telefonnummer und E-Mail-Adresse; 7° Daten, die das Kontaktzentrum benötigt, um weiteren sachdienlichen Kontakt mit der in vorliegendem Paragraphen erwähnten Person aufzunehmen, und Liste der Personen, mit denen die in vorliegendem Paragraphen erwähnte Person in letzter Zeit Kontakt hatte, einschließlich Postleitzahl und Sprache der in vorliegendem Paragraphen erwähnten Person; 8° Liste der Personengemeinschaften, denen die in vorliegendem Paragraphen erwähnte Person angehört oder mit denen sie in Kontakt gekommen ist, und deren Daten von der Datenbank IV mitgeteilt werden; 9° relevante Kriterien zur Bewertung des hohen oder niedrigen Infektionsrisikos und zur Erteilung von Empfehlungen, einschließlich möglicher Symptome, Zeitpunkt des Auftretens der Symptome, Art des verschriebenen COVID–19-Coronavirustests, Arztbesuch und Erfassung der eventuellen Verweigerung eines Arztbesuchs; 10° relevante Daten, die dem Kontaktzentrum von der in vorliegendem Paragraphen erwähnten Person in Bezug auf durchgeführte

Ortswechsel, Symptome und Einhaltung der Isolations-, Präventions- und Hygienemaßnahmen mitgeteilt wurden; 11° bloße Tatsache, dass ein Kontakt zwischen der Person der Kategorie IV und Personen der Kategorien I, II und III stattgefunden hat, einschließlich der Tatsache, dass sie dem Haushalt der Person der Kategorie IV angehören; 12° Antwort auf die Frage, ob (i) [positiv getestete Personen], (ii) Personen der Kategorie III oder (iii) Personen der Kategorie IV eine digitale Kontaktrückverfolgungsanwendung benutzen oder nicht » (Artikel 6 § 5).

Dieselbe Bestimmung sieht vor, dass diese Daten von den Kontaktzentren übermittelt werden.

B.15.6. Für die positiv getesteten Personen der Kategorie II, für die Personen der Kategorien III und IV sowie für die Personen, die einem Cluster angehören, enthält die Datenbank I ebenfalls: « alle Daten, die für Organisation und Rückverfolgung des Kontakts mit der betreffenden Person durch die Mitarbeiter des Kontaktzentrums erforderlich sind, wie zum Beispiel Sprache der betreffenden Person, Kontaktstatus der betreffenden Person, Ticketnummern der Kontaktaufnahmen oder -versuche, Art der Kontakte, Uhrzeit der Tickets, Zeitpunkt und Dauer des Kontakts und Ergebnis des Kontakts » (Artikel 6 §§ 6 und 7).

Für die positiv getesteten Personen der Kategorie II und für die Personen der Kategorien III und IV werden diese Daten von den Kontaktzentren übermittelt (Artikel 6 § 6). Für die Personen, die einem Cluster angehören, werden diese Daten von den zuständigen mobilen Teams oder Gesundheitsinspektionsdiensten übermittelt (Artikel 6 § 7).

B.16.1. Die in den Datenbanken II, III und IV enthaltenen Kategorien von personenbezogenen Daten sind in den Artikeln 7 bis 9 des Zusammenarbeitsabkommens vom 25. August 2020 aufgezählt.

B.16.2. Die Datenbank II enthält daher für die Personen der Kategorien I, II und III « die in Artikel 6 aufgelisteten personenbezogenen Daten […], jedoch nur nach Pseudonymisierung », das heißt: « 1° einmalige Nummer, anhand deren die Person nicht identifiziert werden kann; 2° Geburtsjahr und gegebenenfalls Sterbejahr und Sterbemonat; 3° Geschlecht; 4° Postleitzahl; 5° LIKIV-Nummer des Verschreibers des COVID–19-Coronavirustests; 6° Art, Datum, Testnummer und Ergebnis des COVID–

19-Coronavirustests oder Verdachtsdiagnose, wenn kein COVID–19-Coronavirustest erfolgte; 7° LIKIV-Nummer des Labors, das den COVID–19-Coronavirustest durchgeführt hat; 8° im Falle eines negativen COVID–19- Coronavirustestergebnisses,mögliche Entscheidung eines Arztes, sich darüber hinwegzusetzen; 9° im Falle einer Hinwegsetzung über ein negatives Testergebnis, LIKIV-Nummer des Arztes, der die Entscheidung, sich über das Testergebnis hinwegzusetzen, getroffen hat; 10° gegebenenfalls Art und Postleitzahl der Personengemeinschaft, der die Person angehört oder mit der sie in Kontakt gekommen ist; 11° Ergebnis der ärztlichen Untersuchungen, einschließlich Ergebnis des CT-Scans, 12° Angabe der Ausübung oder Nicht-Ausübung des Berufs eines Gesundheitsdienstleisters; 13° relevante Daten für die Kontaktrückverfolgung, einschließlich Symptome, Datum der ersten Symptome, Ortswechsel und Einhaltung der Isolations- und Hygienemaßnahmen; 14° bloße Tatsache, dass ein Kontakt zwischen der Person der Kategorie IV und einerseits Personen der Kategorie II, insofern der COVID–19-Coronavirustest ergeben hat, dass sie infiziert sind, und andererseits Personen der Kategorie III stattgefunden hat, einschließlich der Tatsache, dass sie dem Haushalt der Person der Kategorie IV angehören » (Artikel 9 § 1).

Für die Personen der Kategorie IV enthält die Datenbank II « die in Artikel 6 aufgelisteten personenbezogenen Daten […], jedoch nur nach Pseudonymisierung », das heißt: « 1° einmalige Nummer, anhand deren die Person nicht identifiziert werden kann; 2° Geburtsjahr und gegebenenfalls Sterbejahr und Sterbemonat; 3° Geschlecht; 4° Symptome; 5° Kontakt oder kein Kontakt mit schutzbedürftigen Personen; 6° Ergebnis und Datum des verschriebenen COVID–19-Coronavirustests; 7° Ausübung des Berufs eines Gesundheitsdienstleisters; 8° unbedingt erforderliche Daten in Bezug auf die Kontaktnahme einschließlich Datum des Tickets und allgemeines Ergebnis der Kontaktaufnahme in Form eines Codes; 9° relevante Kriterien zur Bewertung des hohen oder niedrigen Risikos; 10° Postleitzahl der Adresse » (Artikel 9 § 2).

B.16.3. Die Datenbank III enthält folgende Kategorien von personenbezogenen Daten von positiv getesteten Personen der Kategorie II und von Personen der Kategorie III: « 1° ENSS; 2° Namen und Vornamen; 3° Geschlecht; 4° Geburtsdatum; 5° Kontaktangaben, einschließlich Adresse, Telefonnummer und E-Mail-Adresse der betreffenden Person und der im Notfall zu kontaktierenden Personen; 6° Daten, die das Kontaktzentrum benötigt, um einen sachdienlichen Kontakt mit der betreffenden Person herzustellen, einschließlich Postleitzahl und Sprache; 7° Angabe, dass die Person als (vermutlich) infizierte Person angerufen werden

muss, um ihre Kontakte zurückzuverfolgen; 8° gegebenenfalls Ergebnis des COVID–19-Coronavirustests und Datum des Tests; 9° Ticketnummer, Datum, Uhrzeit und Ergebnis der Kontaktaufnahme » (Artikel 7 § 2).

Für die Personen der Kategorie IV enthält die Datenbank III: « 1° ENSS; 2° Namen und Vornamen; 3° Geschlecht; 4° Geburtsdatum und gegebenenfalls Sterbedatum; 5° Adresse; 6° Kontaktangaben, einschließlich Telefonnummer und E-Mail-Adresse; 7° Daten, die das Kontaktzentrum benötigt, um weiteren sachdienlichen Kontakt mit der in vorliegendem Paragraphen erwähnten Person aufzunehmen, und Liste der Personen, mit denen die in vorliegendem Paragraphen erwähnte Person in letzter Zeit Kontakt hatte, einschließlich Postleitzahl und Sprache der in vorliegendem Paragraphen erwähnten Person; 8° Liste der Personengemeinschaften, denen die in vorliegendem Paragraphen erwähnte Person angehört oder mit denen sie in Kontakt gekommen ist, und deren Daten von der Datenbank IV mitgeteilt werden; 9° relevante Kriterien zur Bewertung des hohen oder niedrigen Infektionsrisikos und zur Erteilung von Empfehlungen, einschließlich möglicher Symptome, Zeitpunkt des Auftretens der Symptome, Art des verschriebenen COVID–19-Coronavirustests, Arztbesuch und Erfassung der eventuellen Verweigerung eines Arztbesuchs; 10° relevante Daten, die dem Kontaktzentrum und den mobilen Teams von der in vorliegendem Paragraphen erwähnten Person in Bezug auf durchgeführte Ortswechsel, Symptome und Einhaltung der Isolations-, Präventions- und Hygienemaßnahmen mitgeteilt wurden; 11° bloße Tatsache, dass ein Kontakt zwischen der Person der Kategorie IV und einerseits Personen der Kategorie II, insofern der COVID–19-Coronavirustest ergeben hat, dass sie infiziert sind, und andererseits Personen der Kategorie III stattgefunden hat, einschließlich der Tatsache, dass sie dem Haushalt der Person der Kategorie IV angehören » (Artikel 7 § 3).

Für die Personen der Kategorie VI enthält die Datenbank III: « 1° Namen, Art und Kontaktinformationen der Personengemeinschaft; 2° Kontaktinformation des Referenzarztes und/oder des Verwaltungsverantwortlichen der Personengemeinschaft, einschließlich Name, Vorname und Telefonnummer » (Artikel 7 § 4).

B.16.4. Die Datenbank IV enthält folgende Kategorien von personenbezogenen Daten von Personen der Kategorien V und VI: « 1° Identifizierungsnummer aus einer authentischen Quelle, insbesondere dem Nationalregister oder der Zentralen Datenbank der sozialen Sicherheit, und interne Identifizierungsnummer; 2° Namen, Art, Adresse und in der Zentralen

Datenbank der Unternehmen aufgeführte Nummer der Personengemeinschaft, der die Person angehört oder mit der sie in Kontakt gekommen ist; 3° Kontaktinformation des Referenzarztes und/oder des Verwaltungsverantwortlichen der Personengemeinschaft, einschließlich Name, Vorname und Telefonnummer » (Artikel 8).

c) Die Kategorien von Personen, die Zugang zu den Daten haben

B.17.1. Aus Artikel 2 §§ 4 und 5 des Zusammenarbeitsabkommens vom 25. August 2020 geht hervor, dass die jeweiligen Verantwortlichen auf die Datenbanken I bis IV zugreifen können, das heißt: Sciensano für die Datenbanken I und II und die zuständigen föderierten Teilgebiete oder ihre Agenturen für die Datenbanken III und IV.

B.17.2. Außerdem haben nach Artikel 10 § 1 Absatz 1 des Zusammenarbeitsabkommens die Kontaktzentren nur « Zugang zu den in Artikel 7 § 2, § 3 und § 4 erwähnten Kategorien von personenbezogenen Daten », das heißt zu den personenbezogenen Daten der Datenbank III der positiv getesteten Personen der Kategorie II und der Personen der Kategorien III, IV und VI.

Nach Artikel 10 § 1 Absatz 2 verfolgt der Zugang der Kontaktzentren zu den Daten der Datenbank III die « in Artikel 3 § 1 Nr. 1 bis 3 und Artikel 3 § 2 erwähnten [Zwecke] », das heißt den Zweck der manuellen Kontaktrückverfolgung und den Zweck der Prävention.

B.17.3. Nach Artikel 10 § 2 des Zusammenarbeitsabkommens haben die zuständigen mobilen Teams und Gesundheitsinspektionsdienste nur « zu den in Artikel 3 § 1 Nr. 3 erwähnten Zwecken », das heißt: für den Zweck der Prävention, Zugang « zu den in Artikel 6 erwähnten Kategorien von personenbezogenen Daten von Personen der Kategorien I, II, III und IV und, wenn erforderlich, der Kategorien V und VI in der Datenbank I ».

B.17.4. Artikel 10 § 3 erster Satz des Zusammenarbeitsabkommens bestimmt, dass personenbezogene Daten der Datenbank I nach Pseudonymisierung der Datenbank II « zu den in Artikel 3 § 1 Nr. 4 bestimmten Zwecken », das heißt für den Zweck der wissenschaftlichen Forschung, zugeführt werden.

B.17.5. Aus dem Vorstehenden ergibt sich, dass neben dem Zugang, den ihr jeweiliger Verantwortlicher hat, auch die zuständigen mobilen Teams und Gesundheitsinspektionsdienste Zugriff auf die Datenbank I haben, während auf die Datenbank III die Kontaktzentren Zugriff haben.

d) Die maximale Aufbewahrungsfrist der Daten

B.18.1. Gemäß dem Grundsatz der Begrenzung der Aufbewahrung der Daten müssen die personenbezogenen Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Artikel 5 Absatz 1 Buchstabe e der DSGVO).

B.18.2. Gemäß Artikel 15 § 1 des Zusammenarbeitsabkommens vom 25. August 2020 werden die in der Datenbank I enthaltenen Daten spätestens sechzig Tage nach ihrer Speicherung gelöscht. Dieselbe Bestimmung sieht vor, dass die in der Datenbank III gespeicherten Daten täglich gelöscht werden.

Artikel 15 § 3 bestimmt, dass die Datenbanken I und III von dem für die Verarbeitung Verantwortlichen spätestens fünf Tage nach Veröffentlichung des königlichen Erlasses zur Erklärung der Beendigung des Zustands der COVID-19-Epidemie « deaktiviert und aufgehoben oder gelöscht » werden.

B.19.1. In Bezug auf die maximale Aufbewahrungsfrist der in der Datenbank II gespeicherten pseudonymisierten personenbezogenen Daten sah Artikel 15 § 2 des Entwurfs des Zusammenarbeitsabkommens vor, dass diese Daten « gemäß den Bestimmungen des Gesetzes vom 10. April 2014 zur Festlegung verschiedener Bestimmungen im Bereich Gesundheit und des zu dessen Ausführung zwischen dem LIKIV und Sciensano abgeschlossenen Zusammenarbeitsabkommens » gelöscht würden.

Nach der Stellungnahme der Datenschutzbehörde Nr. 64/2020 vom 20. Juli 2020 (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/002, S. 23) sieht der letztlich angenommene Artikel 15 § 2 des Zusammenarbeitsabkommens vom 25. August 2020 vor, dass diese Daten « gemäß der für die Aufbewahrung von Gesundheitsakten und im Rahmen der

wissenschaftlichen Forschung im Gesundheitsbereich allgemein angenommenen Frist gelöscht [werden], das heißt nach dreißig Jahren ».

B.19.2. Wenn die klagenden Parteien im zehnten Teil des einzigen Klagegrunds beanstanden, dass in Artikel 15 § 2 des Zusammenarbeitsabkommens vom 25. August 2020 die Aufbewahrungsfrist der in der Datenbank II gespeicherten pseudonymisierten Daten nicht mit der erforderlichen Klarheit präzisiert ist, beziehen sie sich auf den Entwurf des Zusammenarbeitsabkommens und nicht auf das Zusammenarbeitsabkommen. Da sie sich auf eine falsche Annahme stützen, ist der zehnte Teil des einzigen Klagegrunds unbegründet.

B.20.1. Nach Artikel 15 §§ 1 und 3 zweiter Satz des Zusammenarbeitsabkommens werden personenbezogene Daten der Datenbank IV den im Bereich der Erkennung von infektiösen Krankheiten zuständigen föderierten Teilgebieten spätestens fünf Tage nach Veröffentlichung des königlichen Erlasses zur Erklärung der Beendigung des Zustands der COVID-19-Epidemie übertragen.

Für in der Datenbank IV gespeicherte personenbezogene Daten ist keine maximale Aufbewahrungsfrist festgelegt.

B.20.2. Artikel 15 § 1 des Entwurfes des Zusammenarbeitsabkommens bestimmte:

« […] Die personenbezogenen Daten der Datenbank IV werden entweder alle 10 Jahre aktualisiert oder gelöscht […] ».

In Ihrem Gutachten Nr. 67.719/VR vom 15. Juli 2020 zu dem Gesetzesvorentwurf, der zu dem angefochtenen Gesetz vom 9. Oktober 2020 geführt hat, hatte die Gesetzgebungsabteilung des Staatsrates zu dieser Bestimmung angegeben, dass das Fehlen einer maximalen Aufbewahrungsfrist der in der Datenbank IV enthaltenen personenbezogenen Daten nicht mit der DSGVO im Einklang stehe:

« L'article 15, § 1er, alinéa 1er, de l'accord de coopération prévoit que les données à caractère personnel de la Base de données IV sont soit mises à jour tous les dix ans, soit supprimées. Interrogés à cet égard, les délégués ont répondu ce qui suit :

' Na een termijn van 10 jaar worden de gegevens ofwel gewist, ofwel nagekeken op hun accuraatheid en indien nodig geüpdatet. Indien in geval van niet-accurate gegevens updaten

onmogelijk is of niet opportuun, zullen de gegevens gewist worden. Zolang ze niet gewist zijn, zijn ze accuraat en zijn dit de gegevens van de contactpersonen van de collectiviteiten. In geval van uitbraken van andere infectieziekten, zal dit immers zeer nuttig zijn ’.

Cette absence de délai maximal de conservation pour ces données à caractère personnel n’est toutefois pas conforme à l’article 5, paragraphe 1, e), du RGDP, qui prescrit que ‘ les données à caractère personnel doivent être […] conservées sous une forme permettant l’identification des personnes concernées pendant une durée n’excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ’.

39.2. Interrogés quant aux motifs justifiant l’exception envisagée au paragraphe 1er, alinéa 2, pour ce qui concerne les données des Bases de données IV et V, les délégués ont répondu ce qui suit :

‘ Het komt opportuun voor om deze Gegevensbank [IV] te en voortbestaan na de COVID19 crisis. Immers, deze Gegevensbank zal ook haar nut in de toekomst bewijzen. Daarenboven bevat het merendeel van deze gegevens geen persoonsgegevens, maar gegevens over de collectiviteiten zelf ’.

Le dispositif sera revu de manière à rendre celui-ci conforme au principe selon lequel il appartient au législateur de fixer les délais de conservation des données à caractère personnel » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, SS. 55-56).

B.20.3. In den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 25. August 2020 heißt es:

« Les données à caractère personnel de la Base de données III seront supprimées quotidiennement et celles de la Base de données IV sont soit mises à jour, soit supprimées en permanence. Dans l’hypothèse où la mise à jour de données inexactes est impossible ou inappropriée, les données seront supprimées. Tant qu’elles ne sont pas supprimées, elles sont exactes et constituent les données des personnes de contact des collectivités qui seront sauvegardées. Les données à caractère personnel de la Base de données IV seront transférées 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 aux entités fédérées pour l’exécution de leur compétence en matière de détection des maladies infectieuses et contagieuses dans le cadre de leur compétence matérielle en matière de médecine préventive les soins de santé préventifs. En cas d’apparition d’autres maladies infectieuses, la conservation des données à caractère personnel exactes dans la Base de données IV sera en effet très utile. En outre, la Base de données IV ne contient des données à caractère personnel que dans une mesure limitée » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, S. 105).

B.20.4. Die Datenbank IV enthält mehrere Kategorien von personenbezogenen Daten der Personen der Kategorien V und VI. Diese Daten sind in dem vorerwähnten Artikel 8 des Zusammenarbeitsabkommens vom 25. August 2020 aufgezählt.

Dadurch, dass sie keine maximale Aufbewahrungsfrist dieser personenbezogenen Daten vorsehen, verstoßen die Artikel 2 § 3 und 15 §§ 1 und 3 zweiter Satz des Zusammenarbeitsabkommens vom 25. August 2020, wie sie durch die angefochtenen Akte gebilligt wurden, gegen die Artikel 10, 11 und 22 der Verfassung in Verbindung mit Artikel 5 Absatz 1 Buchstabe e der DSGVO.

B.21. Vorbehaltlich der in B.20.4 erwähnten teilweisen Nichtigerklärung bestimmt Artikel 2 des Zusammenarbeitsabkommens vom 25. August 2020 in Verbindung mit seinen Artikeln 1, 3, 6 bis 10 und 15 die in der Datenbank I und in den mit ihr verbundenen Datenbanken II, III und IV verarbeiteten Datenkategorien, die betroffenen Personenkategorien, die mit der Verarbeitung verfolgten Zwecke, die Personenkategorien, die Zugang zu den verarbeiteten Daten haben, und die maximale Aufbewahrungsfrist der Daten. Gemäß Artikel 3 § 4 ist außerdem die Verwendung der erhobenen Daten zu anderen als den in B.14.2 erwähnten Zwecken untersagt.

Die Personen, deren personenbezogene Daten in der Datenbank I und den mit ihr verbundenen Datenbanken gesammelt werden, können daher in ausreichend präziser Weise die Bedingungen kennen, unter denen ihre Daten verarbeitet werden.

2. Die Notwendigkeit und die Verhältnismäßigkeit der Einmischung

B.22. Der Gerichtshof prüft nun die Notwendigkeit und die Verhältnismäßigkeit der Einmischung.

Im Rahmen dieser Prüfung ist zu prüfen, ob der Eingriff nicht über das hinausgeht, was zur Erreichung der verfolgten Ziele erforderlich ist und insbesondere, ob es Maßnahmen gibt, die weniger stark in die betreffenden Rechte eingreifen und trotzdem den Zielen der in Rede stehenden Regelung wirksam dienen (EuGH, 17. Oktober 2013, C-291/12, *Schwarz gegen Stadt Bochum*, Randnrn. 46 und 47). Der Schutz des Grundrechts auf Achtung des Privatlebens auf der Ebene der Union erfordert es nach ständiger Rechtsprechung des Gerichtshofs der Europäischen Union, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken (EuGH, 16. Dezember 2008, C-73/07, *Satakunnan Markkinapörssi und Satamedia*, Randnr. 56; 8. April 2014, C-293/12 und

C-594/12, *Digital Rights Ireland u.a.*, Randnrn. 51 und 52; 6. Oktober 2015, C-362/14, *Schrems*, Randnr. 92, 21. Dezember 2016, C-203/15 und C-698/15, *Tele2 Sverige und Watson u.a.*, Randnrn. 96 und 103; 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u.a.*, Randnr. 130).

Bei der Beurteilung der Verhältnismäßigkeit von Maßnahmen in Bezug auf die Verarbeitung personenbezogener Daten sind u.a. deren automatisierter Charakter, die verwendeten Techniken, der Genauigkeitsgrad, die Relevanz, der gegebenenfalls übermäßige Charakter der zu verarbeitenden Daten, das etwaige Vorhandensein von Maßnahmen zur Begrenzung der Datenspeicherfrist, das etwaige Vorhandensein eines unabhängigen Überwachungssystems, mit dem geprüft werden kann, ob eine Datenspeicherung weiterhin erforderlich ist, das etwaige Vorhandensein von ausreichenden Kontrollrechten und Rechtsbehelfen für die betroffenen Personen, das etwaige Vorhandensein von Garantien zur Vermeidung einer Stigmatisierung der Personen, deren Daten verarbeitet werden, und das etwaige Vorhandensein von Garantien zur Vermeidung einer falschen Nutzung und von Missbrauch der verarbeiteten personenbezogenen Daten durch öffentliche Behörden zu berücksichtigen (Entscheid Nr. 108/2016 vom 14. Juli 2016, B.12.2; Entscheid Nr. 29/2018 vom 15. März 2018, B.14.4; Entscheid Nr. 27/2020 vom 20. Februar 2020, B.8.3; EuGHMR, Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, § 59; Entscheidung, 29. Juni 2006, *Weber und Saravia gegen Deutschland*, § 135; 2. April 2009, *K.H. u.a. gegen Slowakei*, §§ 60-69; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, §§ 101-103, 119, 122 und 124; 18. April 2013, *M.K. gegen Frankreich*, §§ 37 und 42-44; 18. September 2014, *Brunet gegen Frankreich*, §§ 35-37; 12. Januar 2016, *Szabó und Vissy gegen Ungarn*, § 68; EuGH, Große Kammer, 8. April 2014, C-293/12, *Digital Rights Ireland Ltd*, und C-594/12, *Kärntner Landesregierung u.a.*, Randnrn. 56-66).

B.23. Wie in B.1.1 und B.1.3 erwähnt, zielt das Zusammenarbeitsabkommen vom 25. August 2020 auf den Schutz der Volksgesundheit mithilfe einer manuellen und digitalen Kontaktrückverfolgung im Rahmen der Bekämpfung der Ausbreitung von COVID-19 ab.

Dieses Ziel stellt ein legitimes Ziel dar, das Einmischungen in das Recht auf Achtung des Privatlebens und in das Recht auf Schutz personenbezogener Daten rechtfertigen kann. Im Übrigen trägt der Schutz der Volksgesundheit ebenfalls zum Schutz der Rechte und Freiheiten anderer bei.

B.24.1. Aufgrund des Grundsatzes der Datenminimierung müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Artikel 5 Absatz 1 Buchstabe c der DSGVO).

B.24.2. In ihrer Stellungnahme Nr. 42/2020 vom 25. Mai 2020 zu dem Gesetzesvorschlag « zur Schaffung einer Datenbank bei Sciensano im Rahmen der Bekämpfung der Ausbreitung des Coronavirus COVID-19 », der in B.1.4 zitiert wurde, hat die Datenschutzbehörde angemerkt, dass die Zentralisierung einer erheblichen Menge an Gesundheitsdaten « in einer einzigen Datenbank, die von einem Akteur geschaffen, besessen und verwaltet wird, der nur als Vermittler dient » nicht mit diesem Grundsatz übereinstimmt:

« Rien n'indique qu'il soit requis d'effectuer une centralisation de ces données dans une banque de données détenue par un tiers (Sciensano), une telle centralisation n'étant dès lors pas conforme aux principes de nécessité, proportionnalité et minimisation et donc pas acceptable.

[…]

L'Autorité rappelle que la désignation de Sciensano en tant que responsable du traitement […] implique qu'elle soit en charge du respect de toutes les obligations qui s'imposent aux responsables du traitement en vertu du GDPR (fourniture de l'information adéquate aux personnes concernées, mise en place d'un système de gestion des droits des personnes concernées, mise en œuvre de mesures de sécurité appropriées, analyse de risques etc). La portée de cette désignation devrait par ailleurs être précisée. Sciensano n'agit en effet en tant que responsable du traitement que pour ce qui concerne les opérations précitées de collecte, enregistrement dans la banque de données et communication des données à des tiers. Pas pour ce qui concerne les opérations dites ' de traçage ' (prise de contact avec les personnes infectées et leurs contacts) proprement dites.

En ce qui concerne ces opérations, ce sont les agences régionales (qui chapeautent les centres de contact) qui sont responsables de traitement et l'Autorité rappelle également qu'ils sont tenus, à ce titre, de mettre en place les mesures de sécurité, le droit d'accès du citoyen, d'effectuer une analyse de risques etc (article 35).

[…]

La proposition de loi prévoit une centralisation d'une grande quantité de données, essentiellement médicales et donc sensibles, entre les mains d'un acteur unique qui n'est pourtant pas l'acteur qui se chargera de l'accomplissement des trois finalités prévues; Sciensano n'est en effet :

a. pas en charge des opérations visant à contacter les personnes infectées (ou présumées infectées), opérations effectuées par des centres de contact sous la responsabilité des agences régionales compétentes en matière de santé;

b. pas en charge de la réalisation des études épidémiologiques visées à l'article 1§ 2°;

c. et pas non plus mandaté pour effectuer des ' initiatives visant à combattre la propagation des effets nocifs causés par les maladies infectieuses '

L'Autorité se demande pourquoi chacun des acteurs chargés de l'accomplissement de ces finalités ne pourrait pas lui-même collecter et enregistrer les données nécessaires à ces opérations, quitte à les fournir directement aux organismes de recherche épidémiologiques et de santé publique visés par la proposition de loi.

Par ailleurs, l'Autorité ne saisit pas la raison pour laquelle les données relatives aux ' malades ' (personnes présumées infectées par le virus, ayant effectué un test, s'étant vu prescrire un test ou hospitalisées avec un diagnostic confirmé) et celles relatives aux personnes avec lesquelles elles sont entrées en contact doivent être consignées dans la même banque de données (sachant que les secondes sont ' communiquées par les centres de contact ' qui détiennent donc déjà ces données pour contacter ces personnes et n'ont donc pas besoin qu'elles soient enregistrées chez Sciensano – art 2 § 4 de la proposition de loi).

Cette centralisation d'une quantité importante de données relatives à la santé dans une banque de données unique constituée, détenue et gérée par un acteur qui ne ferait office que d'intermédiaire […] n'est pas conforme aux principes de nécessité et de minimisation […] » (SS. 8-10; im selben Sinne: Stellungnahme Nr. 34/2020 vom 28. April 2020 « bezüglich eines Vorentwurfes eines königlichen Erlasses Nr. XXX zur Ausführung von Artikel 5 § 1 Nr. 1 des Gesetzes vom 27. März 2020 zur Ermächtigung des Königs, Maßnahmen zur Bekämpfung der Ausbreitung des Coronavirus COVID-19 zu ergreifen (II) im Rahmen der Nutzung von digitalen Anwendungen zur Kontaktrückverfolgung als Präventionsmaßnahme gegen die Ausbreitung des Coronavirus COVID-19 in der Bevölkerung », S. 5, Stellungnahme Nr. 36/2020 vom 29. April 2020 zum Vorentwurf des königlichen Erlasses, der zum königlichen Erlass Nr. 18 vom 4. Mai 2020 geworden ist, SS. 5 und 11).

B.24.3. Aus den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 25. August 2020 geht hervor, dass die Schaffung einer zentralen Datenbank bei Sciensano mit der Notwendigkeit, in Anbetracht der Mobilität der Bürger eine einheitliche manuelle Ermittlung in ganz Belgien sicherzustellen, mit dem Bestreben, die Arbeitsweise der Kontaktzentren nicht zu verlangsamen, und dem Bestreben, das Risiko von Datenverlusten zu reduzieren, gerechtfertigt wurde:

« Afin de rendre le traitement des données de ce suivi manuel des contacts uniforme dans toute la Belgique, Sciensano, l'Institut belge de santé publique, a été chargé de rassembler les données de santé et les coordonnées des patients auprès des médecins, des laboratoires et des hôpitaux dans une base de données centrale unique.

Une base de données centrale est nécessaire compte tenu de la mobilité des citoyens à travers les différentes entités fédérées. La tenue de différentes bases de données par entité fédérée impliquerait donc une interaction entre ces bases de données dès que de tels

déplacements auraient lieu. Sur le plan pratique, cette interaction pourrait ralentir le fonctionnement des centres de contact puisqu'ils devraient attendre les contributions des autres entités fédérées. En outre, le transfert régulier de données à caractère personnel entre différentes bases de données décentralisées comporte un risque beaucoup plus élevé de fuites des données. Dans l'optique d'une politique plus sûre et plus efficace, l'objectif du présent accord de coopération est avant tout de fournir la base juridique pour cette base de données centrale.

Cette base de données centrale au sein de Sciensano, qui sera mise en place sur la base du présent accord de coopération (ci-après ' Base de données I '), permettra l'échange de données avec les bases de données qui seront créées pour soutenir les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes. Ces dernières, également des bases de données centralisées (ci-après dénommées ' Base de données III et IV '), seront également créées dans le cadre du présent accord de coopération.

L'organisation des bases de données repose sur les principes de protection des données dès la conception et par défaut sur la minimisation des données. Le stockage multiple des mêmes données à caractère personnel dans des bases de données de différentes entités fédérées est évité.

Du point de vue de la technologie de l'information, chaque base de données dispose naturellement de son propre modèle de données sous-jacent. Différents modèles de données donnent lieu à différentes bases de données.

La Base de données I est nécessairement une base de données commune à toutes les entités fédérées car le suivi des contacts ne peut se limiter aux personnes ressortant d'une seule entité fédérée. L'organisation d'une base de données par entité fédérée aurait pour conséquence que chaque région ou communauté devrait gérer sa propre duplication de l'ensemble de la base de données, et il faudrait une synchronisation permanente, avec le risque de fuites de données que cela implique. Ceci est contraire aux principes de minimisation des données et de sécurité des informations prévus dans le Règlement Général sur la Protection des Données.

L'organisation d'une base de données par entité fédérée aurait une incidence négative fondamentale sur le délai d'exécution de l'ensemble du suivi manuel des contacts. En effet, les différentes opérations visant à organiser l'échange de données entre les différentes bases de données des entités fédérées prendraient tellement de temps que cela ralentirait l'ensemble du processus (du suivi des personnes devant passer un test de dépistage du coronavirus COVID-19 à la prise de contact avec les Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID-19 a révélé qu'elles sont infectées, et les Personnes de catégorie III).

La Base de données III est une banque de données distincte qui ne contient que les instructions (d'appel) destinées au personnel des centres de contact. Cette base de données dispose d'un modèle de données différent de la Base de données I et constitue donc une base de données distincte. Du reste, la distinction entre les Bases de données I et III constitue une mesure de protection des données dès la conception qui permet d'éviter que le personnel des centres de contact ne dispose d'un accès indu aux données de santé contenues dans la Base de données I. La Base de données III est une base de données commune aux centres de contact pour la même raison que la Base de données I est une base de données commune aux entités fédérées.

La base de données IV est une base de données distincte contenant des informations sur les collectivités et les personnes de contact des collectivités. Cette base de données dispose d'un modèle de données différent de celui des Bases de données I et III et constitue donc une base de données distincte.

Afin de permettre aux services d'inspection d'hygiène et aux équipes mobiles de remplir correctement les tâches qui leur sont confiées (notamment l'identification et la détection des foyers du coronavirus COVID-19 et clusters, la prise de mesures sur place pour contenir les foyers du coronavirus COVID-19 et les clusters), il est également nécessaire de prévoir un échange de données entre la Base de données I et les services d'inspection d'hygiène, ainsi qu'avec les équipes mobiles » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, SS. 65-69).

B.24.4. In ihrer Stellungnahme Nr. 64/2020 vom 20. Juli 2020 zu dem Entwurf des Zusammenarbeitsabkommens, der zu dem Zusammenarbeitsabkommen vom 25. August 2020 geführt hat, hat die Datenschutzbehörde angegeben, dass die Schaffung einer zentralen Datenbank bei Sciensano unter Berücksichtigung der folgenden Rechtfertigungen notwendig und verhältnismäßig erscheine:

« À ce stade, les justifications avancées dans le commentaire général accompagnant le présent projet semblent justifier la nécessité et la proportionnalité de la création d'une base de données centrale auprès de Sciensano (du moins dans son principe) » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/002, S. 8).

B.24.5. Die Zentralisierung der personenbezogenen Daten in Bezug auf Infektionen mit dem Coronavirus für die Zwecke der Bekämpfung der Ausbreitung von COVID-19 ist im vorliegenden Fall aus Gründen der Sicherheit und der Datenintegrität und der Schnelligkeit der manuellen Rückverfolgung der möglicherweise infizierten Personen gerechtfertigt. Die Zentralisierung der Daten anstelle ihrer Speicherung in getrennten Datenbanken, die von den Kontaktzentren verwaltet werden, bietet mehr Garantien, was ihre Sicherheit und ihre Integrität betreffen. Das Risiko des Missbrauchs und das Risiko von Verzögerungen wären höher, wenn die personenbezogenen Daten in Bezug auf die COVID-19-Infektionen in eine separate Datenbank, die von jedem einzelnen Kontaktzentrum des Landes verwaltet wird, aufgenommen würden.

B.25. Nach Artikel 4 Nummer 7 der DSGVO ist der Verantwortliche « die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das

Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden ».

Der Verantwortliche ist also derjenige, der die Befugnis hat, die Zwecke und Mittel der Verarbeitung der Daten zu bestimmen.

Sciensano erfüllt dieses doppelte Kriterium, was die Verarbeitung der pseudonymisierten personenbezogenen Daten der Datenbank II, die aus der Datenbank I stammen, für den Zweck der wissenschaftlichen Forschung betrifft, angesichts der gesetzlichen Aufträge, mit denen Sciensano durch den vorerwähnten Artikel 4 des Gesetzes vom 25. Februar 2018 « zur Schaffung von Sciensano » betraut ist.

Es geht jedoch aus dem in B.14.2 und B.17 Erwähnten hervor, dass die von den zuständigen föderierten Teilgebieten oder ihren Agenturen bestimmten Kontaktzentren die Verarbeitung von personenbezogenen Daten der Datenbank III, die zum Teil aus der Datenbank I stammen, für den Zweck der manuellen Kontaktrückverfolgung und für den Zweck der Prävention vornehmen, während die mobilen Teams und die Gesundheitsinspektionsdienste der föderierten Teilgebiete die Verarbeitung der Daten der Datenbank I für den Zweck der Prävention vornehmen.

Artikel 26 der DSGVO sieht vor, dass dann, wenn mehrere Verantwortliche die Zwecke der und die Mittel zur Verarbeitung festlegen, sie gemeinsam Verantwortliche sind. Die jeweiligen Pflichten der gemeinsam Verantwortlichen werden in einer Vereinbarung festgelegt (Absatz 1), von der das « Wesentliche » der betroffenen Person zur Verfügung gestellt wird (Absatz 2). Diese kann die Rechte im Rahmen der DSGVO bei jedem einzelnen der Verantwortlichen geltend machen (Absatz 3).

Da die mobilen Teams und die Gesundheitsinspektionsdienste die personenbezogenen Daten der Datenbank I verarbeiten, müssen die zuständigen föderierten Teilgebiete oder ihre Agenturen, unter deren Aufsicht diese Teams und Dienste arbeiten, im Sinne von Artikel 26 der DSGVO als gemeinsam Verantwortliche der Datenbank I neben Sciensano benannt werden. In Anbetracht der engen Verbindungen zwischen den Datenbanken I und III müssen die zuständigen föderierten Teilgebiete oder ihre Agenturen, unter deren Aufsicht die

Kontaktzentren arbeiten, ebenfalls im Sinne von Artikel 26 der DSGVO als gemeinsam Verantwortliche der Datenbank I benannt werden.

B.26. Der erste Teil des einzigen Klagegrunds ist in dem in B.20.4 und in dem in B.25 erwähnten Maße begründet.

Die angefochtenen Akte sind für nichtig zu erklären, insoweit sie einerseits die Artikel 2 § 3 und 15 §§ 1 und 3 zweiter Satz des Zusammenarbeitsabkommens vom 25. August 2020, insofern diese Bestimmungen keine maximale Aufbewahrungsfrist der in der Datenbank IV gespeicherten personenbezogenen Daten vorsehen, und andererseits Artikel 2 § 4 desselben Zusammenarbeitsabkommens, insofern diese Bestimmung nicht vorsieht, dass die zuständigen föderierten Teilgebiete oder ihre Agenturen, unter deren Aufsicht die Kontaktzentren, die mobilen Teams und die Gesundheitsinspektionsdienste arbeiten, gemeinsam Verantwortliche der Datenbank I sind, billigen.

II. In Bezug auf die Notwendigkeit, bestimmte Datenkategorien zu sammeln (zweiter Teil)

B.27. Im zweiten Teil des einzigen Klagegrunds machen die klagenden Parteien geltend, dass die Artikel 6 bis 9 des Zusammenarbeitsabkommens vom 25. August 2020 eine unverhältnismäßige Einmischung in das Recht auf Achtung des Privatlebens und in das Recht auf Schutz personenbezogener Daten zur Folge hat, da diese Bestimmungen die Sammlung von bestimmten nicht für den Zweck der manuellen Kontaktrückverfolgung notwendigen personenbezogenen Daten vorsähen (erster Beschwerdegrund). Außerdem sei die Entscheidung, die verarbeiteten Daten zu Forschungszwecken zu pseudonymisieren, nicht gerechtfertigt (zweiter Beschwerdegrund).

B.28. Die klagenden Parteien machen geltend, dass die Sammlung der Erkennungsnummer der sozialen Sicherheit (nachstehend: ENSS), der personenbezogenen Daten aus dem Nationalregister, des Ergebnisses des CT-Scans und der Sprache der betroffenen Person in der Datenbank I für den Zweck der manuellen Kontaktrückverfolgung nicht notwendig ist. Das Gleiche gelte für die in der Datenbank I gesammelten personenbezogenen Daten bezüglich der Personen der Kategorie III.

B.29.1. Das Zusammenarbeitsabkommen vom 25. August 2020 sieht die Erfassung der ENSS in der Datenbank I für Personen der Kategorien I bis IV vor (Artikel 6 § 2 Absatz 1 Nr. 1, § 3 Nr. 1, § 4 Absatz 4 Nr. 1 und § 5 Nr. 1).

Wie Artikel 1 § 1 Nr. 11 des Zusammenarbeitsabkommens präzisiert, ist die ENSS die Erkennungsnummer im Sinne vom Artikel 8 § 1 Nr. 1 oder Nr. 2 des Gesetzes vom 15. Januar 1990 « über die Errichtung und Organisation einer Zentralen Datenbank der sozialen Sicherheit ». Das ist für natürliche Personen, die im Nationalregister gespeichert sind, die Erkennungsnummer des Nationalregisters und für natürliche Personen, die nicht im Nationalregister gespeichert sind, die Erkennungsnummer der Zentralen Datenbank der sozialen Sicherheit.

Die Entscheidung, die ENSS zu verwenden, wird in den allgemeinen Erläuterungen des Zusammenarbeitsabkommens wie folgt begründet:

« En vue de l'identification univoque des personnes concernées (c'est-à-dire les patients hospitalisés, les personnes infectées ou les personnes sérieusement suspectées d'être infectées) et de la mise en relation des données collectées, il est absolument indispensable de conserver également le numéro d'identification de sécurité sociale des personnes concernées dont les données sont traitées dans la base de données I et de permettre un accès général au Registre national. Cela soulage également les médecins, les hôpitaux et les laboratoires qui mettent les informations à disposition (c'est-à-dire les fournisseurs d'information), car ils n'ont à fournir que les données qui ne figurent pas dans le Registre national. Étant donné que l'ensemble du système de soins de santé en Belgique repose sur l'utilisation du numéro de Registre national pour identifier effectivement un patient, ce numéro est également essentiel pour le traitement dans le cadre du suivi manuel des contacts, en vue d'identifier correctement la personne index ainsi que les personnes avec lesquelles la personne index est entrée en contact. L'inclusion du numéro d'identification de sécurité sociale entraîne nécessairement l'enregistrement de la date de naissance des personnes concernées dont les données sont sauvegardées dans la Base de données I.

L'utilisation obligatoire du numéro d'identification à la sécurité sociale comme numéro d'identification unique dans le secteur des soins de santé est également régie par l'article 8 de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth. Dans son arrêt 29/2010 du 18 mars 2010, la Cour constitutionnelle a estimé que ' [compte] tenu des garanties prévues par la loi du 21 août 2008 quant à la confidentialité des données à caractère personnel relatives à la santé au cours de leur traitement par la plate-forme eHealth, le choix de recourir au numéro du Registre national comme clé d'identification est raisonnablement justifié » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, SS. 82-84).

Die Sammlung der ENSS in der Datenbank I als Erkennungsschlüssel der Personen der Kategorien I bis IV ist daher vernünftig gerechtfertigt.

B.29.2. Artikel 6 § 2 Absatz 2 § 3 Nr. 1 und § 4 Absatz 2 des Zusammenarbeitsabkommens vom 25. August 2020 sieht außerdem vor, dass Name und Vorname, Geschlecht und Adresse der Personen der Kategorien I bis III in der Datenbank I auf der Grundlage des Nationalregisters oder der Register der Zentralen Datenbank der sozialen Sicherheit erfasst werden.

Daraus folgt, dass der Zugang zu diesen Registern es nur ermöglichen darf, personenbezogene Daten zur Identifizierung der (potenziell) infizierten oder vermutlich infizierten Personen zu erfassen, was für die Verwirklichung des Zwecks der manuellen Kontaktrückverfolgung notwendig ist.

B.30.1. Das Zusammenarbeitsabkommen sieht ebenfalls vor, dass « das Ergebnis des CT-Scans » in der Datenbank I für eine Person der Kategorie I, die im Krankenhaus behandelt wird, gesammelt werden kann (Artikel 6 § 2 Absatz 1 Nr. 12), wobei der « CT-Scan » eine Technik der medizinischen Bildgebung bezeichnet. Nach Ansicht der klagenden Parteien verfolgt die Sammlung dieser Kategorie von Daten ausschließlich den Zweck der wissenschaftlichen Forschung und nicht den der manuellen Kontaktrückverfolgung.

B.30.2. Aufgrund des Grundsatzes der Zweckbindung müssen die personenbezogenen Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und die eventuelle Weiterverarbeitung dieser Daten muss mit diesen ursprünglichen Zwecken vereinbar sein (Artikel 5 Absatz 1 Buchstabe b der DSGVO). Gemäß dem Grundsatz der Datenminimierung müssen diese Daten dem Zweck angemessen und erheblich sowie auf das für die verfolgten Zwecke notwendige Maß beschränkt sein (Artikel 5 Absatz 1 Buchstabe c der DSGVO).

B.30.3. In den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 25. August 2020 heißt es:

« Les catégories de données à caractère personnel collectées sont les suivantes : des données d'identification et de contact, données relatives aux tests de dépistage, prescriptions, résultats des examens par CT-scans et diagnostics présumés des personnes, d'une part, et des données relatives aux personnes infectées ou sérieusement suspectées d'être infectées ainsi qu'aux patients hospitalisés dont le diagnostic du coronavirus COVID-19 a été confirmé dans les hôpitaux, d'autre part. […]

En ce qui concerne les tests de dépistage du coronavirus COVID-19, non seulement les résultats des tests de dépistage du coronavirus COVID-19 sont importants, mais le type de test de dépistage du coronavirus COVID-19 prescrit et/ou effectué, ainsi que la date du test de dépistage du coronavirus COVID-19, sont également indispensables. D'une part, pour déterminer si un patient est infecté ou non et, d'autre part, pour permettre aux chercheurs de mener des recherches qualitatives et statistiques supplémentaires sur les tests de dépistage du coronavirus COVID-19. Une infection par le coronavirus COVID-19 peut également être déduite des résultats des examens des CT-scans. La collecte de ces données permet d'obtenir plus de clarté sur l'évolution générale de la maladie du coronavirus COVID-19 chez un patient infecté » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, SS. 81-82).

B.30.4. Daraus geht hervor, dass das Ergebnis einer per CT-Scan durchgeführten Untersuchung ein Element medizinischer Bildgebung ist, das es ermöglicht, bei einem Patienten die Infektion mit dem Coronavirus festzustellen. Vorbehaltlich der Auslegung, dass der in Artikel 6 § 2 Absatz 1 Nr. 12 des Zusammenarbeitsabkommens erwähnte CT-Scan ein CT-Scan ist, aus dem eine COVID-19-Infektion ersichtlich ist, kann angenommen werden, dass die Erfassung dieser Daten in der Datenbank I für die Verwirklichung des Zwecks der Kontaktrückverfolgung notwendig ist, die es erfordert, vorher den Status der mit COVID-19 infizierten Personen festzustellen.

B.31. Das Zusammenarbeitsabkommen sieht außerdem die Speicherung der Sprache der vermutlich infizierten Personen (Personen der Kategorie III) (Artikel 6 § 4 Nr. 12), der Personen, mit denen die positiv getesteten Personen und die vermutlich infizierten Personen in Kontakt waren (Personen der Kategorie IV), der positiv getesteten Personen der Kategorie II (Artikel 6 § 5 Nr. 7 und § 6) und der Personen, die einem Cluster angehören (Artikel 6 § 7), in der Datenbank I vor.

Es kann angenommen werden, dass der Vermerk der Sprache der betroffenen Person notwendig ist, um es den Kontaktzentren zu ermöglichen, mit dieser Person in ihrer Sprache in Kontakt zu treten.

B.32.1. Gemäß Artikel 1 § 1 Nr. 15 des Zusammenarbeitsabkommens vom 25. August 2020 sind die Personen der Kategorie III « Personen, bei denen der Arzt den ernsthaften Verdacht hat, dass sie mit dem Coronavirus COVID–19 infiziert sind, ohne dass ein COVID–19-Coronavirustest durchgeführt oder verschrieben wurde, oder bei denen der COVID–19- Coronavirustest ergeben hat, dass sie nicht infiziert sind ».

Wie in B.15.4 erwähnt, bestimmt Artikel 6 § 4 des Zusammenarbeitsabkommens die personenbezogenen Daten der Personen der Kategorie III, die in der Datenbank I von dem Arzt, der den Verdacht einer Infektion hat, gespeichert werden.

B.32.2. In ihrer vorerwähnten Stellungnahme Nr. 64/2020 vom 20. Juli 2020 hat die Datenschutzbehörde angemerkt:

« 42. Le projet prévoit la collecte et l'enregistrement, dans la Base de données I, de données à caractère personnel concernant des personnes présumées infectées (personnes de catégorie III). Si, dans un premier temps, au vu de la pénurie de tests permettant de confirmer une infection au coronavirus, il a pu sembler justifié de se contenter d'une forte présomption pour établir l'existence d'une infection au COVID-19, l'Autorité se demande si tel est toujours le cas aujourd'hui alors que les capacités de testing ont été très largement augmentées depuis le début de l'épidémie et qu'il apparait qu'aujourd'hui toutes les personnes pour lesquelles on suspecte une infection au COVID-19 devraient pouvoir être testées. L'Autorité se demande dès lors pourquoi le projet prévoit une collecte et un enregistrement de nombreuses données concernant les personnes présumées infectées dans la base de données I (et III).

43. Par ailleurs, comme l'Autorité a déjà eu l'occasion de le souligner dans ses avis n° 36/2020 et n° 42/2020, la donnée ' diagnostic présumé de contamination par le coronavirus COVID-19 ' peut difficilement être considérée comme une donnée exacte au sens de l'article 5.1.d) du RGPD » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/002, S. 17).

B.32.3. In den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 25. August 2020 heißt es:

« Un patient pour lequel il existe un soupçon sérieux qu'il est infecté par le coronavirus COVID-19, est un patient dont le médecin a déclaré que même sans test le patient présente des symptômes suffisants pour supposer l'infection ou dont le test de dépistage du coronavirus COVID-19 a montré que le patient n'est pas infecté, mais que le médecin ignore cette décision. Comme les deux diagnostics de soupçon de contamination sont établis par un médecin et sont donc suffisamment fiables, il est nécessaire d'également désigner ces personnes présumées infectées en tant que personnes infectées et de les inclure dans la recherche de contacts. Le terme de personnes présumées infectées fait donc référence aux personnes désignées par un médecin comme personnes index mais qui n'ont pas été officiellement désignées comme infectées par un test » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, S. 84).

B.32.4. Die Einbeziehung von vermutlich infizierten Personen in das System der manuellen Kontaktrückverfolgung wurde so mit der Verlässlichkeit der vom Arzt erstellten Diagnose gerechtfertigt. Um die Volksgesundheit bei der COVID-19-Pandemie zu schützen, konnten die Gesetzgeber in die manuelle Kontaktrückverfolgung Personen einbeziehen, bei

denen ein Arzt einen starken klinischen Verdacht hat, ohne dass ein Test durchgeführt wurde oder trotz des negativen Testergebnisses, dass sie infiziert sind.

Im Übrigen ergibt sich aus Artikel 3 § 1 Nr. 1 und § 2 Nr. 1 des Zusammenarbeitsabkommens vom 25. August 2020, dass die Verarbeitung von personenbezogenen Daten bezüglich der Personen der Kategorie III in der Datenbank I entgegen den Ausführungen der klagenden Parteien sehr wohl den Zweck der manuellen Kontaktrückverfolgung und nicht nur den Zweck der wissenschaftlichen Forschung verfolgt.

B.33. Was die Entscheidung, die zu Forschungszwecken verarbeiteten Daten zu pseudonymisieren betrifft, werden in Artikel 9 des Zusammenarbeitsabkommens die Kategorien von personenbezogenen Daten der Datenbank I aufgezählt, die nach Pseudonymisierung in der Datenbank II gespeichert werden, um zu wissenschaftlichen Forschungszwecken verwendet zu werden.

Zu diesem Punkt heißt es in den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen:

« […] il convient de continuer à garantir les fonctions de recherche épidémiologique existante. Il importera donc, sur la base des données fournies dans le cadre du suivi manuel des contacts de permettre aux institutions de recherche, y compris Sciensano, d'effectuer des études scientifiques ou statistiques liées à la propagation du coronavirus COVID-19 et/ou de soutenir la politique de lutte contre le coronavirus, grâce à l'échange de données entre la Base de données I et la base de données déjà en place au sein de Sciensano, laquelle est utilisée actuellement pour la recherche scientifique (ci-après ' Base de données II '). C'est une tâche qui relève de la compétence matérielle de l'État fédéral en matière de recherche scientifique. Le traitement des données à caractère personnel dans la Base de données I s'inscrit également dans le cadre des compétences fédérales en matière de recherche scientifique, comme il ressort de l'article 1er, § 2 de l'accord de coopération. À ce titre, il s'inscrit dans le cadre des missions confiées à Sciensano par l'article 4 de la loi du 25 février 2018 ' portant création de Sciensano '. Seul l'échange de données à caractère personnel pseudonymisées dans le cadre de la recherche scientifique avec la base de données déjà existante de Sciensano (Base de données II) est donc régi par l'accord de coopération. L'établissement de règles relatives à la mise en œuvre de la recherche scientifique même ne relève donc pas du champ d'application de l'accord de coopération.

En ce qui concerne cet échange de données, on opte pour la pseudonymisation plutôt que pour l'anonymisation car il n'est pas possible de déterminer préalablement quelles données sont nécessaires pour mener une recherche scientifique particulière. Il semble donc approprié de ne pas priver les données de leur valeur potentielle lorsqu'elles sont enregistrées dans la Base de données II, mais aussi de protéger autant que possible les données à caractère personnel des

personnes concernées. Comme l'a souligné le Comité européen de la protection des données, le nouveau concept de pseudonymisation tel que défini pour la première fois dans le Règlement Général sur la Protection des Données constitue un mécanisme de protection approprié. Ce concept de pseudonymisation impose également de prendre des mesures techniques et organisationnelles appropriées, conformes à la minimisation des données et à la protection des données dès la conception. La plateforme eHealth sera responsable dans ce cadre de la pseudonymisation des données à caractère personnel. Cette pseudonymisation a lieu lorsque et avant que les données à caractère personnel de la Base de données I sont partagées avec la Base de données II. Il n'est donc pas question de données pseudonymisées dans la Base de données I, parce que cela n'est pas techniquement faisable et parce qu'il convient toujours de satisfaire aux principes imposés par le Règlement Général sur la Protection des Données » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, SS. 69-71).

Daraus geht hervor, dass die Entscheidung, die in der Datenbank II gespeicherten personenbezogenen Daten zu pseudonymisieren anstatt sie zu anonymisieren, vernünftig gerechtfertigt ist.

B.34. Vorbehaltlich der in B.30.4 erwähnten Auslegung ist der zweite Teil des einzigen Klagegrunds unbegründet.

III. In Bezug auf die dem Informationssicherheitsausschuss erteilte Ermächtigung, die Mitteilung von personenbezogenen Daten an Dritte zu genehmigen (dritter Teil)

B.35.1. Im dritten Teil des einzigen Klagegrunds machen die klagenden Parteien geltend, dass die Artikel 11 und 12 des Zusammenarbeitsabkommens vom 25. August 2020 gegen das in Artikel 22 der Verfassung enthaltene Legalitätsprinzip verstoßen, insofern sie den Informationssicherheitsausschuss ermächtigten, die wesentlichen Elemente im Zusammenhang mit der Mitteilung von personenbezogenen Daten an Dritte festzulegen. Nach Auffassung der klagenden Parteien können die Beschlüsse des Informationssicherheitsausschusses nicht als ein « Gesetz » im Sinne von Artikel 6 Absatz 2, Artikel 9 Absatz 2 Buchstabe i) und Artikel 9 Absatz 4 der DSGVO angesehen werden. Außerdem könne die Genehmigungsbefugnis des Informationssicherheitsausschusses nicht auf der Grundlage von Artikel 36 Absatz 5 der DSGVO gerechtfertigt werden, da dieser Ausschuss nicht als eine Aufsichtsbehörde angesehen werden könne.

B.35.2. Der Beschwerdegrund der klagenden Parteien bezieht sich nur auf die Befugnisübertragung an den Informationssicherheitsausschuss in Bezug auf die Mitteilung von

personenbezogenen Daten an Dritte. Diese Maßnahme ist in Artikel 11 § 1 des Zusammenarbeitsabkommens vom 25. August 2020 in Verbindung mit seinem Artikel 10 § 3 zweiter Satz vorgesehen.

Der Gerichtshof beschränkt seine Prüfung auf diese Bestimmungen.

B.36.1. Artikel 11 § 1 des Zusammenarbeitsabkommens vom 25. August 2020 bestimmt:

« Soweit eine entsprechende Mitteilung nicht in vorliegendem Zusammenarbeitsabkommen vorgesehen ist, erfolgen sowohl die Mitteilung von personenbezogenen Daten je nach Akteurtyp an Sciensano zur Verarbeitung in der Datenbank I als auch die weitere Mitteilung dieser personenbezogenen Daten von Sciensano an Dritte wie in Artikel 10 vorgesehen immer nach Beschlussfassung der Kammer Soziale Sicherheit und Gesundheit des Informationssicherheitsausschusses wie erwähnt im Gesetz vom 5. September 2018 zur Schaffung des Informationssicherheitsausschusses und zur Abänderung verschiedener Gesetze zur Ausführung der Datenschutz-Grundverordnung ».

Artikel 10 § 3 zweiter Satz bestimmt :

« Personenbezogene Daten wie mitgeteilt und gespeichert in der Datenbank II dürfen Dritten nur zu den in Artikel 3 § 1 Nr. 4 erwähnten Zwecken und nach einer in Artikel 11 erwähnten Beschlussfassung der Kammer Soziale Sicherheit und Gesundheit des Informationssicherheitsausschusses übermittelt werden ».

Artikel 3 § 1 Nr. 4 bestimmt:

« Die Verarbeitung personenbezogener Daten in der Datenbank I dient folgenden Verarbeitungszwecken:

[…]

4° Zurverfügungstellung pseudonymisierter personenbezogener Daten, die gemäß den Bestimmungen von Artikel 10 unter die in Artikel 6 erwähnten Kategorien von personenbezogenen Daten von Personen der Kategorien I bis V fallen, an die bereits bestehende Datenbank II, um die in vorliegendem Absatz erwähnten pseudonymisierten Daten nach Anonymisierung, oder zumindest nach Pseudonymisierung, wenn die Anonymisierung es den Forschungseinrichtungen nicht erlauben würde, ihre wissenschaftliche oder statistische Studie durchzuführen, Forschungseinrichtungen, einschließlich Sciensano, gemäß dem zu diesem Zweck vorgesehenen Verfahren zur Verfügung zu stellen, um den Forschungseinrichtungen zu ermöglichen, wissenschaftliche oder statistische Studien über die Bekämpfung der Ausbreitung des Coronavirus COVID–19 durchzuführen und/oder, nach Pseudonymisierung, die Politik in diesem Bereich gemäß Titel 4 des Gesetzes vom 30. Juli 2018 über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten zu unterstützen ».

B.36.2. Artikel 11 § 1 des Zusammenarbeitsabkommens vom 25. August 2020 in Verbindung mit seinem Artikel 10 § 3 zweiter Satz ermächtigt die Kammer « Soziale Sicherheit und Gesundheit » des Informationssicherheitsausschusses, im Wege von Beschlüssen die Mitteilung von « zu den in Artikel 3 § 1 Nr. 4 bestimmten Zwecken », das heißt zu wissenschaftlichen Forschungszwecken, pseudonymisiert in der Datenbank II gespeicherten personenbezogenen Daten an Dritte zu genehmigen.

B.36.3. In Bezug auf die in den Artikeln 10 § 3 und 11 § 1 des Entwurfs des Zusammenarbeitsabkommens enthaltene Ermächtigung hat die Datenschutzbehörde folgende Anmerkungen gemacht:

« 58. L'article 10 § 3 du projet prévoit que ' […] Les données à caractère personnel telles que communiquées et conservées dans la Base de données II, ne peuvent être transmises à des tiers aux fins stipulées à l'article 3, § 1, 4° qu'après la délibération, visée à l'article 11, de la Chambre " Sécurité sociale et Santé " du Comité de sécurité de l'information '. L'Autorité rappelle qu'aux termes des principes de transparence et de légalité, la norme encadrant une communication de données – en tout cas lorsque celle-ci […] constitue une ingérence importante dans les droits et libertés des personnes concernées – doit déterminer les destinataires ou, en tout cas, les catégories de destinataires auxquelles ces données peuvent être communiquées. Les auteurs du projet devraient dès lors identifier, à tout le moins, les catégories de tiers auxquels ces données peuvent être communiquées.

59. L'article 11 § 1er du projet prévoit que ' Dans la mesure où cela n'est pas repris dans le présent accord de coopération, tant la communication de données à caractère personnel à Sciensano pour traitement dans la Base de données I que la communication ultérieure de ces données à caractère personnel par Sciensano à des tiers ont toujours lieu après délibération de la Chambre " Sécurité sociale et Santé " du Comité de sécurité de l'information visé dans la loi du 5 septembre 2018 instituant le Comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement Général sur la Protection des Données '.

60. L'Autorité rappelle, comme elle l'a déjà fait dans ses avis n^{os} 36/2020 et 42/2020, que ni l'article 8 de la CEDH, ni l'article 22 de la Constitution, ni le RGPD, en particulier l'article 6.3, ne permettent un tel ' chèque en blanc '. Comme l'Autorité l'a déjà souligné plus haut, tout traitement (y compris donc toute communication) de données à caractère personnel susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, comme c'est le cas, en l'espèce, doit être encadré spécifiquement par un texte législatif ou réglementaire (arrêté), et donc pas par une délibération du Comité de sécurité de l'information. L'Autorité rappelle que cette règlementation doit être précise et définir, au moins, les éléments essentiels du traitement, dont les finalités déterminées, explicites et légitimes; les (catégories de) données à caractère personnel qui sont pertinentes, adéquates et limitées à ce qui est nécessaire au regard des finalités poursuivies; le délai de conservation maximal des données à caractère personnel enregistrées; la désignation du responsable du traitement; les destinataires

ou catégories de destinataires auxquels les données sont communiquées et les circonstances dans lesquelles et les raisons pour lesquelles elles seront communiquées.

61. L'accord de coopération doit donc déterminer lui-même quels sont les ' tiers ' à qui Sciensano peut communiquer des données qu'il désigne et les raisons pour lesquelles ces données leur seront communiquées. Certainement au vu de la quantité et de la sensibilité des données en question (données relatives à la santé, données relatives à une présomption d'infection suite à un contact) et de la possibilité pour leurs destinataires potentiels d'effectuer des recoupements entre ces différents types de données » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/002, SS. 21-22).

B.36.4. In den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 25. August 2020 heißt es:

« Les données pseudonymisées contenues dans la Base de données II ne peuvent être transférées à des tiers que dans le cadre d'études scientifiques ou statistiques relatives à [la] lutte contre la propagation du coronavirus COVID-19 et/ou pour soutenir les politiques dans ce domaine. Ce transfert n'est possible qu'après délibération de la Chambre ' sécurité sociale et santé ' du Comité de sécurité de l'information » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, SS. 93-94).

« Une délibération de la Chambre ' sécurité sociale et santé ' du Comité de sécurité de l'information est aussi requise pour l'échange des données de la Base de données II avec des tiers à des fins de recherche scientifique. Toutefois, l'octroi d'accès à des tiers pour la recherche scientifique ne relève pas du champ d'application de l'accord de coopération et ne sera donc pas traité plus en détail dans le présent accord de coopération » (ebenda, SS. 96-97).

B.37.1. Wie in B.11.2 erwähnt, garantiert Artikel 22 der Verfassung, indem er dem zuständigen Gesetzgeber die Befugnis vorbehält, festzulegen, in welchen Fällen und unter welchen Bedingungen das Recht auf Achtung des Privat- und Familienlebens beeinträchtigt werden kann, jedem Bürger, dass eine Einmischung in dieses Recht nur aufgrund von Regeln erfolgen darf, die durch eine demokratisch gewählte beratende Versammlung angenommen wurden.

Eine Ermächtigung einer anderen Gewalt steht nicht im Widerspruch zum Legalitätsprinzip, sofern die Ermächtigung ausreichend präzise umschrieben ist und sich auf die Ausführung von Maßnahmen bezieht, deren wesentliche Elemente vorher durch den Gesetzgeber festgelegt worden sind.

B.37.2. Artikel 6 Absatz 2 der DSGVO bestimmt, dass die Mitgliedstaaten « spezifischere Bestimmungen » zur Anpassung der Anwendung der Vorschriften der DSGVO in Bezug auf

eine Verarbeitung, die zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist (Artikel 6 Absatz 1 Buchstabe c), und eine Verarbeitung, die für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, erforderlich ist (Artikel 6 Absatz 1 Buchstabe e), beibehalten oder einführen können. Artikel 9 Absatz 2 Buchstabe i der DSGVO sieht vor, dass das Unionsrecht oder das Recht eines Mitgliedstaats, auf dessen Grundlage die Verarbeitung sensibler Daten aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich ist, « angemessene und spezifische Maßnahmen » zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht. Artikel 9 Absatz 4 sieht vor, dass die Mitgliedstaaten « zusätzliche Bedingungen, einschließlich Beschränkungen, » einführen oder aufrechterhalten können, soweit die Verarbeitung von Gesundheitsdaten betroffen ist.

Artikel 36 Absatz 5 bestimmt, dass Verantwortliche durch das Recht der Mitgliedstaaten verpflichtet werden können, bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung zu Zwecken der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren und deren vorherige Genehmigung einzuholen.

B.38.1. Der Informationssicherheitsausschuss wurde durch Artikel 2 § 1 des Gesetzes vom 5. September 2018 « zur Schaffung des Informationssicherheitsausschusses und zur Abänderung verschiedener Gesetze zur Ausführung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG » (nachstehend: Gesetz vom 5. September 2018) geschaffen. Im Gegensatz zu den sektoriellen Ausschüssen, die durch das Gesetz vom 3. Dezember 2017 « zur Schaffung der Datenschutzbehörde » abgeschafft wurden, denen er nachfolgt und die in den früheren Ausschuss für den Schutz des Privatlebens integriert waren, wurde der Informationssicherheitsausschuss auf der Grundlage der vorerwähnten Artikel 6 Absatz 2 und Artikel 9 Absatz 4 der DSGVO als ein neues von der Datenschutzbehörde unabhängiges Organ eingerichtet (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3185/001, SS. 6-7 und 30; DOC 54-3185/005, SS. 7-10). Aus den Vorarbeiten zum Gesetz vom 5. September 2018 geht hervor, dass der Gesetzgeber gewollt hat, dass der Informationssicherheitsausschuss weder als ein Verantwortlicher noch als eine Aufsichtsbehörde im Sinne der DSGVO angesehen wird (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3185/001, SS. 8-10).

Gemäß Artikel 2 § 2 des Gesetzes vom 5. September 2018 besteht der Informationssicherheitsausschuss aus zwei Kammern: einer Kammer « Soziale Sicherheit und Gesundheit » und einer Kammer « Föderalbehörde ». Die Artikel 2 § 1 und 4 § 1 Absatz 1 desselben Gesetzes bestimmen, dass seine Mitglieder von der Abgeordnetenkammer, die sie auch von ihrem Auftrag entbinden kann, für einen erneuerbaren Zeitraum von sechs Jahren ernannt werden. Artikel 5 desselben Gesetzes bestimmt, dass die Mitglieder des Informationssicherheitsausschusses « […] von niemandem Weisung [erhalten] ». Aus den Vorarbeiten geht hervor, dass der Gesetzgeber wollte, dass der Informationssicherheitsausschuss keinerlei hierarchischer Kontrolle unterliegt (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3185/001, S. 10).

Die Befugnis, administrative Entscheidungen zu treffen, die der Kammer « Soziale Sicherheit und Gesundheit » des Informationssicherheitsausschusses durch Artikel 11 § 1 des Zusammenarbeitsabkommens vom 25. August 2020 in Verbindung mit seinem Artikel 10 § 3 zweiter Satz erteilt wird (die Mitteilung von personenbezogenen Daten zu genehmigen oder abzulehnen), entspricht der Befugnis, die dieser Kammer durch Artikel 15 § 1 Absatz 1 des Gesetzes vom 15. Januar 1990 « über die Errichtung und Organisation einer Zentralen Datenbank der sozialen Sicherheit », ersetzt durch Artikel 18 des Gesetzes vom 5. September 2018, durch Artikel 42 § 2 Nr. 3 des Gesetzes vom 13. Dezember 2006 « zur Festlegung verschiedener Bestimmungen im Bereich Gesundheit », abgeändert durch Artikel 43 des Gesetzes vom 5. September 2018, und durch Artikel 11 des Gesetzes vom 21. August 2008 « zur Einrichtung und Organisation der eHealth-Plattform und zur Festlegung verschiedener Bestimmungen », abgeändert durch Artikel 50 des Gesetzes vom 5. September 2018, erteilt wird. Mit diesen Bestimmungen wird die Kammer « Soziale Sicherheit und Gesundheit » des Informationssicherheitsausschusses ermächtigt, jeweils (1) die Mitteilung von sozialen personenbezogenen Daten durch die Zentrale Datenbank der sozialen Sicherheit oder durch eine Einrichtung für soziale Sicherheit an eine andere Einrichtung für soziale Sicherheit oder eine andere Stelle als einen föderalen öffentlichen Dienst, einen öffentlichen Programmierungsdienst oder eine föderale Einrichtung öffentlichen Interesses, (2) die Mitteilung von personenbezogenen Gesundheitsdaten und (3) die Mitteilung von personenbezogenen Daten durch oder an die Plattform eHealth zu genehmigen. In Ausübung ihrer Genehmigungsbefugnis beschränken sich die Kammern des Informationssicherheitsausschusses darauf zu prüfen, dass bei der fraglichen Mitteilung von

personenbezogenen Daten die Grundsätze der Zweckbindung, der Verhältnismäßigkeit und der Sicherheit, die in der DSGVO festgelegt sind, eingehalten werden (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3185/001, SS. 6, 8 und 9).

Artikel 46 § 2 Absatz 1 des Gesetzes vom 15. Januar 1990 « über die Errichtung und Organisation einer zentralen Datenbank der sozialen Sicherheit », ersetzt durch Artikel 39 des Gesetzes vom 5. September 2018, bestimmt, dass die Beschlüsse des Informationssicherheitsausschusses « allgemeinverbindlich zwischen den Parteien und gegenüber Dritten » sind. Laut den Vorarbeiten zum Gesetz vom 5. September 2018 haben diese Beschlüsse « normativen Wert (Gesetz im materiellen Sinne) gemäß der verfassungsmäßigen Ordnung und können durch die geltenden Rechtsmittel angefochten werden, wenn sie im Widerspruch zu übergeordneten Rechtsnormen stehen » (ebenda, S. 8). Absatz 2 desselben Bestimmung lautet:

« Die Datenschutzbehörde kann die Beschlüsse des Informationssicherheitsausschusses jederzeit auf die Entsprechung mit höheren Rechtsnormen prüfen, unabhängig davon, wann sie gefasst wurden. Wenn sie unter Angabe von Gründen feststellt, dass ein Beschluss einer höheren Rechtsnorm nicht entspricht, kann sie unbeschadet ihrer sonstigen Befugnisse den Informationssicherheitsausschuss auffordern, diesen Beschluss zu den von ihr angegebenen Punkten binnen fünfundvierzig Tagen und ausschließlich für die Zukunft neu zu erwägen. Gegebenenfalls legt der Informationssicherheitsausschuss der Datenschutzbehörde den geänderten Beschluss zur Stellungnahme vor. Sofern sie nicht binnen fünfundvierzig Tagen weitere Bemerkungen formuliert, gilt der geänderte Beschluss als endgültig ».

Artikel 46 § 1 Nr. 8 des Gesetzes vom 15. Januar 1990« über die Errichtung und Organisation einer zentralen Datenbank der sozialen Sicherheit », ersetzt durch Artikel 39 des Gesetzes vom 5. September 2018, bestimmt außerdem, dass der Informationssicherheitsausschuss jährlich auf der Website der Zentralen Datenbank und auf der Website der eHealth-Plattform einen kurzen Bericht über die Erfüllung ihrer Aufträge im vergangenen Jahr veröffentlicht. Schließlich heißt es in den Vorarbeiten zum Gesetz vom 5. September 2018, dass gegen die Beschlüsse des Informationssicherheitsausschusses Klage vor dem Staatsrat erhoben werden kann (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3185/001, SS. 10 und 31).

B.38.2. Aus dem Vorstehenden geht hervor, dass die Beschlüsse des Informationssicherheitsausschusses insbesondere für die Personen verbindlich sind, deren Verarbeitung von personenbezogenen Daten von diesem Ausschuss genehmigt wird. Diese

Beschlüsse unterliegen einer schwachen Kontrolle durch die Datenschutzbehörde, denn diese kann den Informationssicherheitsausschuss lediglich auffordern, einen Beschluss « neu zu erwägen », den sie für unrechtmäßig hält, und eine Stellungnahme zu dem nach dieser Aufforderung geänderten Beschluss abgeben. Zwar wird den betroffenen Personen nicht eine gerichtliche Beschwerde gegen die Beschlüsse des Informationssicherheitsausschusses entzogen, aber ihnen wird die Garantie entzogen, dass diese der parlamentarischen Kontrolle unterliegen. Weder die Ernennung und die Entbindung der Mitglieder des Informationssicherheitsausschusses durch die Abgeordnetenkammer noch die Verpflichtung zur jährlichen Veröffentlichung eines kurzen Berichts über die Erfüllung der Aufträge des Informationssicherheitsausschusses auf der Website der Zentralen Datenbank und auf der Website der eHealth-Plattform kommen nämlich einer solchen Kontrolle gleich.

B.39. Wie die Gesetzgebungsabteilung des Staatsrates in ihrem Gutachten Nr. 63.202/2 vom 26. April 2018 über den Gesetzesvorentwurf, der zum Gesetz vom 5. September 2018 geworden ist, angemerkt hat, « schreibt die DSGVO die Unabhängigkeit der Aufsichtsbehörde und nicht die der öffentlichen Behörden vor, die – während sie nicht die Rechtsstellung einer solchen Aufsichtsbehörde erhalten – die personenbezogenen Daten verarbeiten oder solche Verarbeitungen genehmigen und eben gerade der Kontrolle der Aufsichtsbehörde unterworfen sein müssen » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3185/001, S. 129). Die Bestimmungen, Maßnahmen und Bedingungen, die die Mitgliedstaaten aufgrund von Artikel 6 Absatz 2, Artikel 9 Absatz 2 Buchstabe i und Artikel 9 Absatz 4 der DSGVO erlassen können, ändern nichts an dieser Feststellung.

Indem er die Kammer « Soziale Sicherheit und Gesundheit » des Informationssicherheitsausschusses, dessen Rechtsstellung nicht durch das Gesetz präzisiert ist und dessen Beurteilungsbefugnis auch nicht durch das Gesetz eingegrenzt ist, ermächtigt, Beschlüsse auf dem Gebiet der Verarbeitung von personenbezogenen Daten zu treffen, die für Dritte bindend sind, ohne dass solche Beschlüsse einer parlamentarischen Kontrolle unterworfen werden können, entzieht Artikel 11 § 1 des Zusammenarbeitsabkommens vom 25. August 2020 in Verbindung mit seinem Artikel 10 § 3 zweiter Satz den betroffenen Personen die Garantie einer solchen Kontrolle, ohne dass dies durch ein Erfordernis gerechtfertigt ist, das sich aus dem Recht der Europäischen Union ergibt.

Die Gesetzgeber haben außerdem wesentliche Elemente der in B.36.2 erwähnten Mitteilung von personenbezogenen Daten an Dritte übertragen, indem sie die Empfänger dieser Mitteilung nicht bestimmt haben.

B.40. Die angefochtenen Akte sind für nichtig zu erklären, insoweit sie das Zusammenarbeitsabkommen vom 25. August 2020 billigen, insofern sein Artikel 11 § 1 die Wörter « sowohl » und « als auch die weitere Mitteilung dieser personenbezogenen Daten von Sciensano an Dritte wie in Artikel 10 vorgesehen » enthält, und insoweit sie Artikel 10 § 3 zweiter Satz desselben Zusammenarbeitsabkommens billigen.

IV. In Bezug auf die durch die Kontaktzentren den behandelnden Ärzten zur Verfügung gestellte Information (vierter Teil)

B.41. Im vierten Teil des einzigen Klagegrunds beanstanden die klagenden Parteien, dass Artikel 3 § 1 Nr. 2 Buchstabe B des Zusammenarbeitsabkommens vom 25. August 2020 vorsieht, dass die behandelnden Ärzte über den Gesundheitszustand der Personen der Kategorien II und III ohne Einwilligung der betroffenen Personen informiert werden.

B.42. Die behandelnden Ärzte der Personen der Kategorien I, II und III sind die Personen der Kategorie V im Sinne von Artikel 1 § 1 Nr. 17 des Zusammenarbeitsabkommens vom 25. August 2020. Zwar war diese Personenkategorie ursprünglich in Artikel 3 § 1 Nr. 2 Buchstabe B des Entwurfs des Zusammenarbeitsabkommens erwähnt, aber sie ist nicht mehr in Artikel 3 § 1 Nr. 2 Buchstabe B des letztlich angenommenen Zusammenarbeitsabkommens vom 25. August 2020 aufgeführt, der bestimmt:

« Die Verarbeitung personenbezogener Daten in der Datenbank I dient folgenden Verarbeitungszwecken:

[…]

B. Zurverfügungstellung der in Artikel 7 § 4 bestimmten Kategorien von personenbezogenen Daten durch die Datenbank I an das zuständige Kontaktzentrum durch einen Austausch mit der Datenbank III, um mit den Personen der Kategorie VI auf jedem möglichen Kommunikationsweg, einschließlich per Telefon, E-Mail oder durch einen Besuch der Personengemeinschaft, in Kontakt zu treten, um sie über die (vermutete) Infektion (i) von

Personen der Kategorie II, insofern der COVID–19-Coronavirustest ergeben hat, dass diese Personen infiziert sind, und (ii) von Personen der Kategorie III zu informieren ».

Die « Personen der Kategorie VI » sind gemäß Artikel 1 § 1 Nr. 18 desselben Zusammenarbeitsabkommens der « Referenzarzt oder, in Ermangelung eines Referenzarztes bei der betreffenden Personengemeinschaft, [der Verwaltungsverantwortliche] der Personengemeinschaften, mit denen Personen der Kategorie I, II und III während eines Zeitraums von vierzehn Tagen vor und vierzehn Tagen nach den ersten Symptomen der Infektion mit dem Coronavirus COVID–19 Kontakt hatten, wobei auf der Grundlage wissenschaftlicher Erkenntnisse ein gewisser Ermessensspielraum berücksichtigt werden kann ».

B.43. Insofern er auf einer falschen Prämisse beruht, ist der vierte Teil des einzigen Klagegrunds unbegründet.

V. In Bezug auf den Zweck der wissenschaftlichen Forschung (fünfter Teil)

B.44. Im fünften Teil des einzigen Klagegrunds machen die klagenden Parteien geltend, dass Artikel 3 § 1 Nr. 4 des Zusammenarbeitsabkommens vom 25. August 2020 gegen den Grundsatz der Zweckbindung und den Grundsatz der Datenminimierung verstößt, insofern der Zweck der wissenschaftlichen Forschung fälschlicherweise als primärer Zweck der Verarbeitung und nicht als ein weiterer Zweck angesehen werde.

B.45. Der in Artikel 5 Absatz 1 Buchstabe b der DSGVO erwähnte Grundsatz der Zweckbindung hat zwei Bestandteile. Er erfordert es einerseits, dass die personenbezogenen Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden, und andererseits, dass diese Daten nicht « in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden ». Dieselbe Bestimmung sieht vor, dass « eine Weiterverarbeitung […] für wissenschaftliche […] Forschungszwecke […] gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken [gilt] ».

B.46. Artikel 3 § 1 Nr. 4 des Zusammenarbeitsabkommens bestimmt:

« Die Verarbeitung personenbezogener Daten in der Datenbank I dient folgenden Verarbeitungszwecken:

[…]

4° Zurverfügungstellung pseudonymisierter personenbezogener Daten, die gemäß den Bestimmungen von Artikel 10 unter die in Artikel 6 erwähnten Kategorien von personenbezogenen Daten von Personen der Kategorien I bis V fallen, an die bereits bestehende Datenbank II, um die in vorliegendem Absatz erwähnten pseudonymisierten Daten nach Anonymisierung, oder zumindest nach Pseudonymisierung, wenn die Anonymisierung es den Forschungseinrichtungen nicht erlauben würde, ihre wissenschaftliche oder statistische Studie durchzuführen, Forschungseinrichtungen, einschließlich Sciensano, gemäß dem zu diesem Zweck vorgesehenen Verfahren zur Verfügung zu stellen, um den Forschungseinrichtungen zu ermöglichen, wissenschaftliche oder statistische Studien über die Bekämpfung der Ausbreitung des Coronavirus COVID–19 durchzuführen und/oder, nach Pseudonymisierung, die Politik in diesem Bereich gemäß Titel 4 des Gesetzes vom 30. Juli 2018 über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten zu unterstützen ».

B.47.1. Wie in B.14 erwähnt, stellt die wissenschaftliche Forschung den dritten Zweck der Verarbeitung personenbezogener Daten in der Datenbank I dar. Aus dieser Bestimmung und aus dem verfügenden Teil des Zusammenarbeitsabkommens vom 25. August 2020 geht hervor, dass die Daten der Datenbank I jedoch nicht unmittelbar für die wissenschaftliche Forschung verwendet werden. Sie werden zu diesem Zweck erst in einem zweiten Schritt verarbeitet, nachdem sie in der Datenbank II in pseudonymisierter Form gespeichert wurden.

Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken, die aufgrund des Zusammenarbeitsabkommens vom 25. August 2020 vorgenommen wird, stellt daher eine « Weiterverarbeitung » von Daten im Sinne von Artikel 5 Absatz 1 Buchstabe b der DSGVO dar. Gemäß derselben Bestimmung gilt diese Weiterverarbeitung als mit den ursprünglichen Zwecken der Verarbeitung vereinbar, die im vorliegenden Fall der Zweck der manuellen Kontaktrückverfolgung und der Zweck der Prävention sind.

B.47.2. Entgegen den Ausführungen der klagenden Parteien bedeutet der Umstand, dass die im Zusammenarbeitsabkommen vom 25. August 2020 vorgesehene Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken eine Weiterverarbeitung von Daten ist, nicht, dass sich diese Verarbeitung auf die Einwilligung der betroffenen Person stützen muss.

Wie es im Erwägungsgrund Nr. 50 der DSGVO heißt, ist im Fall einer mit den ursprünglichen Zwecken vereinbaren Weiterverarbeitung « keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten ». Daraus folgt, dass die Grundlagen für die Rechtmäßigkeit, auf die sich die Erfassung der personenbezogenen Daten in der Datenbank I für die ursprünglichen Zwecke der manuellen Kontaktrückverfolgung und der Prävention stützt, ebenfalls als Grundlage für die Rechtmäßigkeit der Weiterverarbeitung dieser Daten zu wissenschaftlichen Forschungszwecken nach Pseudonymisierung dienen. Im vorliegenden Fall können diese Grundlagen für die Rechtmäßigkeit sowohl die lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person (Artikel 6 Absatz 1 Buchstabe d), die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Artikel 6 Absatz 1 Buchstabe e), die Gesundheitsvorsorge (Artikel 9 Absatz 2 Buchstabe h) als auch Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (Artikel 9 Absatz 2 Buchstabe i) sein.

B.47.3. Was den Beschwerdegrund der klagenden Parteien, dass die im Zusammenarbeitsabkommen vom 25. August 2020 vorgesehene Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken dazu führe, dass nicht für die Verwirklichung des Zwecks der manuellen Kontaktrückverfolgung erforderliche Daten erhoben würden, betrifft, wird auf die Prüfung des zweiten Teils des einzigen Klagegrunds verwiesen.

B.48. Der fünfte Teil des einzigen Klagegrunds ist unbegründet.

VI. In Bezug auf die Verbindungen zwischen der Datenbank I und der Datenbank V und den Begriff der « Risikokontakte » (sechster und siebter Teil)

B.49. Im sechsten und siebten Teil des einzigen Klagegrunds machen die klagenden Parteien geltend, dass Artikel 14 des Zusammenarbeitsabkommens vom 25. August 2020 gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten verstößt, insofern er nicht vorsehe, dass die in der Datenbank I enthaltenen Daten ausschließlich für die manuelle Kontaktrückverfolgung und nicht für die digitale Kontaktrückverfolgung bestimmt seien, und insofern er den Begriff des « Risikokontakts » nicht definiere.

B.50. Wie in B.1.2 und B.13.3 erwähnt, werden in Artikel 14 des Zusammenarbeitsabkommens vom 25. August 2020, der sein Kapitel VIII bildet, die Regeln bezüglich der digitalen Kontaktrückverfolgungsanwendungen festgelegt. Artikel 14 § 3 Nr. 2 sieht die Schaffung der Datenbank V vor, die in Artikel 1 § 1 Nr. 10 als « zentrale Logliste der digitalen Kontaktrückverfolgungsanwendung, die die Kontrolle des Betriebs der digitalen Kontaktrückverfolgungsanwendung, wie in Artikel 14 beschrieben, gewährleistet und die bei Sciensano von den Datenbanken I und II getrennt ist » definiert ist.

B.51.1. Die klagenden Parteien führen zunächst an, dass die Verbindungen zwischen der Datenbank I und der Datenbank V nicht ausreichend klar seien und dass die Datenbank I ebenfalls das Ziel einer digitalen Kontaktrückverfolgung verfolge.

B.51.2. Aus dem vorerwähnten Artikel 1 § 1 Nr. 10 des Zusammenarbeitsabkommens vom 25. August 2020 und seinen allgemeinen Erläuterungen geht hervor, dass die Datenbank I von der Datenbank V getrennt ist und dass Sciensano für die Einhaltung dieser Trennung sorgt. In den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 25. August 2020 heißt es:

« La question de savoir si une application numérique de traçage des contacts est utilisée ou non ne concerne que les données agrégées (c'est-à-dire la réponse affirmative ou négative à cette question) qui ne sont jamais reliées à l'application numérique de traçage des contacts elle-même. Si l'application numérique de traçage des contacts est utilisée par les personnes index et les personnes avec lesquelles ces personnes index ont été en contact, ces dernières ont déjà été informées concernant une contamination potentielle. Ces personnes ont en effet déjà été averties d'une contamination potentielle. L'enregistrement de ces données permet également de vérifier le fonctionnement de l'application numérique de traçage des contacts » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, SS. 89-90).

« L'application mobile de l'application numérique de traçage des contacts enregistre les contacts entre les utilisateurs sans les identifier. La Base de données V permet à un utilisateur de transmettre volontairement et de manière contrôlée une infection identifiée et le moment probable de cette infection, afin que les autres utilisateurs puissent être informés s'ils ont été en contact avec l'utilisateur infecté pendant la période où il a été infecté, sans que l'identité de l'utilisateur infecté ou de l'autre utilisateur avec lequel il a été en contact puisse être identifiée » (ebenda, S. 115).

« Le présent accord de coopération prévoit que Sciensano est le responsable du traitement de la Base de données V. Sciensano doit s'assurer que les mesures techniques et organisationnelles nécessaires ont été prises pour cette base de données, et que les données de

cette base de données ne sont pas croisées avec d'autres bases de données. Compte tenu de l'expérience particulière de Sciensano en matière de protection des données lors du traitement de données de santé pour la recherche scientifique et de la mise en œuvre de telles méthodes de sécurisation et de pseudonymisation des données, Sciensano semble être le responsable le plus approprié pour effectuer ce traitement » (ebenda, SS. 116-117).

Aus den Anmerkungen der beklagten Behörden kann außerdem geschlossen werden, dass der Verweis in Artikel 2 § 1 des Zusammenarbeitsabkommens vom 25. August 2020 auf dessen Artikel 1 § 2 falsch ist und als ein Verweis auf Artikel 1 § 2 Nr. 1 und 3 zu verstehen ist.

Wie in B.13.5 erwähnt, ist die Datenbank I daher nicht mit der Datenbank V verbunden.

B.51.3. Der sechste Teil des einzigen Klagegrunds ist unbegründet.

B.52.1. Die klagenden Parteien führen sodann an, dass Artikel 14 des Zusammenarbeitsabkommens den Begriff « Risikokontakt » nicht definiere.

B.52.2. Der Begriff « Risikokontakt » ist definiert in Artikel 1 Nr. 10 des ausführenden Zusammenarbeitsabkommens vom 13. Oktober 2020 zwischen dem Föderalstaat, der Flämischen Gemeinschaft, der Wallonischen Region, der Deutschsprachigen Gemeinschaft und der Gemeinsamen Gemeinschaftskommission in Bezug auf die digitale(n) Kontaktrückverfolgungsanwendung(en) (nachstehend: ausführendes Zusammenarbeitsabkommen vom 13. Oktober 2020), abgeschlossen gemäß Artikel 92*bis* § 1 Absatz 3 des Sondergesetzes vom 8. August 1980 zur Reform der Institutionen, angenommen in Ausführung von Artikel 14 § 9 Nr. 2 des Zusammenarbeitsabkommens vom 25. August 2020.

Artikel 14 § 9 Nr. 2 des Zusammenarbeitsabkommens vom 25. August 2020 bestimmt:

« Es sind die föderierten Teilgebiete, die beschließen, welche mobile(n) Anwendung(en) im Rahmen der Kontaktrückverfolgung durch die Behörden den Benutzern zur Verfügung gestellt werden, und die Konformität mit den Vorschriften überprüfen. Diesbezügliche Verfahren und der weitere Betrieb der digitalen Kontaktrückverfolgungsanwendung und in diesem Rahmen nützliche Datenverarbeitungen werden unbeschadet der Bestimmungen des vorliegenden Artikels durch ein in Artikel 92*bis* § 1 Absatz 3 des Sondergesetzes vom 8. August 1980 zur Reform der Institutionen erwähntes ausführendes Zusammenarbeitsabkommen geregelt. Dieses ausführende Zusammenarbeitsabkommen umfasst zumindest:

[…]

2° eine deutliche Beschreibung der Verarbeitungen, die aus der Benutzung der digitalen Kontaktrückverfolgungsanwendung hervorgehen, und eine deutliche Bestimmung von bedeutenden Begriffen wie Risikokontakt […] ».

Artikel 1 Nr. 10 des ausführenden Zusammenarbeitsabkommens vom 13. Oktober 2020 bestimmt:

« Für die Anwendung des vorliegenden Abkommens versteht man unter:

[…]

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 ».

B.52.3. Der siebte Teil des einzigen Klagegrunds ist unbegründet.

VII. In Bezug auf den Begriff « physischer Besuch » (achter Teil)

B.53. Im achten Teil des einzigen Klagegrunds machen die klagenden Parteien geltend, dass Artikel 3 § 1 Nr. 2 Buchstabe A und § 2 Nr. 2 Buchstabe A des Zusammenarbeitsabkommens vom 25. August 2020 nicht dem Grundsatz der Zweckbindung genügt, insofern er den Begriff « physischer Besuch » nicht definiere.

B.54.1. Artikel 3 § 1 Nr. 2 A des Zusammenarbeitsabkommens vom 25. August 2020 bestimmt:

« Die Verarbeitung personenbezogener Daten in der Datenbank I dient folgenden Verarbeitungszwecken:

[…]

2° A. Zurverfügungstellung der in Artikel 7 § 3 bestimmten Kategorien von personenbezogenen Daten durch die Datenbank I an das zuständige Kontaktzentrum durch einen Austausch mit der Datenbank III, um mit den Personen der Kategorie IV auf jedem

möglichen Kommunikationsweg, einschließlich per Telefon, E-Mail oder durch einen physischen Besuch, in Kontakt zu treten, um ihnen Empfehlungen hinsichtlich Hygiene und Prävention zu geben, eine Quarantäne vorzuschlagen oder sie aufzufordern, sich auf das Coronavirus COVID–19 testen zu lassen, und in diesem Stadium ein Follow-up anzubieten ».

Artikel 3 § 2 Nr. 2 A bestimmt:

« Die von den zuständigen föderierten Teilgebieten oder den zuständigen Agenturen bestimmten Kontaktzentren dürfen, soweit sie zuständig sind und gemäß Artikel 10 § 1:

[…]

2° A. in Artikel 7 § 3 bestimmte Kategorien von personenbezogenen Daten verarbeiten, um mit Personen der Kategorie IV auf jedem möglichen Kommunikationsweg, einschließlich per Telefon, E-Mail oder durch einen physischen Besuch, in Kontakt zu treten, um ihnen Empfehlungen hinsichtlich Hygiene und Prävention zu geben, eine Quarantäne vorzuschlagen oder sie aufzufordern, sich auf das Coronavirus COVID–19 testen zu lassen, und ein Follow-up anzubieten ».

B.54.2. Wie in B.14.2 erwähnt, sehen diese Bestimmungen vor, dass die Kontaktzentren über einen Datenaustausch zwischen der Datenbank I und der Datenbank III die Kategorien der personenbezogenen Daten der Personen, mit denen die positiv getesteten Personen und die vermutlich infizierten Personen während eines Zeitraums von vierzehn Tagen vor und nach den ersten Anzeichen einer Infektion in Kontakt waren (Personen der Kategorie IV), erhalten, um ihnen Empfehlungen hinsichtlich Hygiene und Prävention zu geben, ihnen eine Quarantäne vorzuschlagen oder sie aufzufordern, sich testen zu lassen. In diesen Bestimmungen ist präzisiert, dass diese Kontaktaufnahme « auf jedem möglichen Kommunikationsweg, einschließlich per Telefon, E-Mail oder durch einen physischen Besuch » erfolgen kann.

Artikel 3 § 1 Nr. 1 und § 2 Nr. 1 des Zusammenarbeitsabkommens vom 25. August 2020 erlaubt es außerdem den Kontaktzentren, insbesondre durch physische Besuche mit den positiv getesteten Personen der Kategorie II und den vermutlich infizierten Personen (Personen der Kategorie III) in Kontakt zu treten, um ihnen eventuelle Empfehlungen zu geben, aber vor allem um sie um Informationen über Personen, zu denen sie Kontakt hatten, zu bitten.

Nach Artikel 1 § 1 Nr. 4 desselben Zusammenarbeitsabkommens ist das Kontaktzentrum die « von den zuständigen föderierten Teilgebieten oder den zuständigen Agenturen bestimmte Instanz, die mit der betreffenden Person im Rahmen der in Artikel 3 § 2 bestimmten Zwecke auf jedem möglichen Kommunikationsweg, einschließlich per Telefon, E-Mail oder durch

einen physischen Besuch, in Kontakt tritt und anschließend die gesammelten Daten mit der Datenbank I teilt ». Nach seinem Artikel 1 § 1 Nr. 20 sind die Felduntersucher die « Mitarbeiter der Kontaktzentren, die im Rahmen der Kontaktermittlung Besuche vor Ort vornehmen können ».

B.54.3. In ihrer vorerwähnten Stellungnahme Nr. 64/2020 vom 20. Juli 2020 hat die Datenschutzbehörde angemerkt:

« 19. Tout d'abord, l'Autorité constate que le projet est beaucoup plus détaillé que les autres projets normatifs sur lesquels elle s'est déjà prononcée. L'Autorité remarque, en effet, que le projet cherche à clarifier, avec un grand degré de précision, les finalités qu'il poursuit, les données qui seront collectées et utilisées, ainsi que les flux de données qui seront mis en place.

20. Certains éléments doivent toutefois encore être clarifiés afin que l'accord de coopération encadre de manière suffisamment prévisible les traitements de données qu'il met en place. C'est, en particulier, le cas pour ce qui concerne les ' visites physiques ' qui pourront avoir lieu dans le contexte du suivi ' manuel ' des personnes (présumées) infectées et de leurs contacts.

21. Le projet entend, en effet, autoriser les ' centres de contact ' compétents à procéder à des ' visites physiques ' auprès des personnes de catégories II dont le test de dépistage du COVID-19 a révélé qu'elles étaient infectées, des personnes de catégories III [c.-à-d. les personnes présumées infectées] et des personnes de catégories IV [c.-à-d. les personnes ayant eu des contacts avec des personnes (présumées) infectées].

22. Actuellement, le projet n'apporte aucun encadrement spécifique de ces ' visites physiques ' qui constituent pourtant une ingérence importante dans le droit au respect de la vie privée des personnes concernées. Il conviendrait, afin que le projet réponde à l'exigence de prévisibilité qui s'impose à toute norme qui permet une interférence avec le droit au respect de la vie privée, que le projet détermine les conditions et les circonstances dans lesquelles une visite physique peut avoir lieu. Il faudrait, en particulier, que le projet détermine :

- les lieux dans lesquels ces visites peuvent avoir lieu (au domicile, sur le lieu de travail, …)

- les heures auxquelles elles peuvent avoir lieu

- les circonstances dans lesquelles elles peuvent avoir lieu, notamment, en indiquant si les centres de contacts doivent d'abord essayer de contacter les personnes concernées par des moyens moins intrusifs

- le caractère contraignant de telles visites. En d'autres termes, les personnes sont-elles contraintes d'ouvrir la porte aux personnes qui se rendraient chez elles (et si oui, des sanctions sont-elles prévues ?) ou ont-elles le choix de refuser d'ouvrir la porte si elles ne souhaitent pas donner des informations aux centres de contact ?

- le déroulement de ces visites et les données, y compris à caractère personnel, qui seront collectées à leur occasion (type de données, personnes concernées etc.)

23. Si la réponse à ces questions se trouvait dans d'autres législations, notamment régionales ou communautaires, il conviendrait de renvoyer explicitement et précisément aux dispositions qui encadrent ces ' visites physiques '. S'il n'existe aucune disposition de droit positif qui encadre de telles ' visites physiques ', il convient de prévoir un tel encadrement afin de permettre aux personnes concernées de connaitre les conditions et les circonstances dans lesquelles de telles visites peuvent avoir lieu.

24. L'Autorité estime que ces visites physiques ne peuvent être effectuées qu'afin de fournir à la personne visitée la même information que celle fournie aux personnes contactées par téléphone et que ces visites ne peuvent donner lieu à un contrôle du respect de recommandations précédemment fournies » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/002, SS. 9-10).

B.55.1. Der von den Felduntersuchern aufgrund der angefochtenen Bestimmung vorgenommene physische Besuch stellt eine Einmischung in das Recht auf Achtung der Wohnung und des Privatlebens dar.

B.55.2. Aus den in B.54 erwähnten Bestimmungen und den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen geht hervor, dass der physische Besuch, der jede Form von Zwang ausschließt, ein subsidiäres Mittel ist, über das die Felduntersucher für die Kontaktaufnahme mit den (vermutlich) infizierten Personen und ihren Kontakten verfügen, um ihnen Empfehlungen hinsichtlich Hygiene und Prävention zu geben, ihnen eine Quarantäne vorzuschlagen oder sie aufzufordern, sich testen zu lassen, wenn eine Kontaktaufnahme per Telefon oder auf elektronischem Wege unmöglich ist. Die Modalitäten zur Durchführung dieser Besuche sind zudem durch die Regelungen der föderierten Teilgebiete festgelegt:

« Le centre de contact contacte non seulement les personnes dont les médecins ont de sérieux soupçons d'infection et celles dont le test de dépistage du coronavirus COVID-19 a révélé qu'elles étaient infectées, notamment les personnes index, mais aussi les personnes avec lesquelles elles ont eu des contacts étroits. Le centre de contact désigné par les entités fédérées compétentes ou par les agences compétentes reçoit ces données de la Base de données I auprès de Sciensano. En cas de contacts avec des personnes au sein d'une population fragile, le centre de contact prendra contact avec le médecin de référence ou, à défaut, avec le responsable administratif de cette collectivité pour un suivi complémentaire de la situation. Dans le cas de contacts avec des personnes individuelles, le centre de contact joint ces personnes par téléphone, leur donne ensuite les recommandations appropriées sur la base des informations qu'elles fournissent (rester chez soi, travailler à domicile, se faire tester, etc.) et confirme ces recommandations par voie électronique. Cet envoi électronique se résume à une confirmation des recommandations transmises oralement. Il est également possible que des enquêteurs de

terrain effectuent des visites physiques aux personnes concernées lorsque le contact téléphonique ou électronique est impossible » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, SS. 91-92).

« Les règles spécifiques relatives à la mise en œuvre du traçage (comme […] les visites à domicile […]) ne relèvent […] pas du champ d'application de l'accord de coopération et sont régies par les réglementations applicables des autorités fédérées » (ebenda, S. 64).

B.55.3. Mit dem Zusammenarbeitsabkommen vom 25. August 2020 soll lediglich ein normativer Rahmen für die gemeinsame Verarbeitung von Daten durch Sciensano, die Kontaktzentren, die Gesundheitsinspektionsdienste und die mobilen Teams im Rahmen der Kontaktrückverfolgung von (vermutlich) mit COVID-19 infizierten Personen und ihrer Kontakte geschaffen werden. Angesichts dieses Ziels machen die in Zusammenarbeitsabkommen und in den allgemeinen Erläuterungen enthaltenen Präzisierungen bezüglich der subsidiären Beschaffenheit des physischen Besuchs gegenüber der Kontaktaufnahme per Telefon und per E-Mail und der von diesen verschiedenen Kontaktmodalitäten verfolgte identische Zweck die Umstände, unter denen ein solcher Besuch von den Felduntersuchern vorgenommen werden kann, ausreichend vorhersehbar. Insoweit die Gemeinschaften es im Rahmen ihrer Zuständigkeit in Angelegenheiten der Gesundheitsvorsorge unterlassen haben sollten, die Regeln bezüglich der Durchführung von physischen Besuchen zu präzisieren, würde sich dieser Umstand nicht aus den angefochtenen Akten ergeben.

B.55.4. Unter Berücksichtigung des in B.55.2 Erwähnten ist der achte Teil des einzigen Klagegrunds unbegründet.

VIII. In Bezug auf die Geheimhaltungspflicht der Mitarbeiter der Kontaktzentren (neunter Teil)

B.56. Im neunten Teil des einzigen Klagegrunds führen die klagenden Parteien an, dass das Zusammenarbeitsabkommen vom 25. August 2020 im Widerspruch zu Artikel 9 Absatz 2 Buchstabe i der DSGVO stehe, insofern es nicht vorsehe, dass die Mitarbeiter der Kontaktzentren dem Berufsgeheimnis unterlägen.

B.57. Wie in B.10.2 erwähnt, sieht Artikel 9 Absatz 2 Buchstabe i der DSGVO vor, dass im Fall der Verarbeitung sensibler Daten, die aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, erlaubt ist, das Recht der Union oder das Recht des Mitgliedstaats angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, « insbesondere des Berufsgeheimnisses », vorsieht.

B.58. In ihrer vorerwähnten Stellungnahme Nr. 64/2020 vom 20. Juli 2020 hat die Datenschutzbehörde angemerkt:

« 25. Les traitements de données envisagés dans le projet portent, en partie, sur des données concernant la santé dont le traitement est, en principe, interdit (article 9.1 du RGPD). Toutefois, cette interdiction ne s'applique pas lorsque – comme c'est le cas en l'espèce – ' le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ' (article 9.2.i) du RGPD).

26. À propos de cette exigence de secret, l'Autorité souligne que l'article 9.3°) de la LTD impose au responsable du traitement de données concernant la santé de veiller à ce que les personnes ayant accès aux données à caractère personnel concernant la santé, qu'il doit désigner, soient ' tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées '. Sauf erreur de l'Autorité, le projet ne crée, par contre, pas d'obligation spécifique de secret dans le chef des personnes (y compris celles travaillant dans les centres de contact) qui auront accès aux données relatives à la santé. Comme l'Autorité l'a déjà indiqué dans son avis n° 36/2020, l'Autorité estime qu'afin de préserver la confidentialité de l'identité et de l'état de santé des personnes identifiables dont les données à caractère personnel seront reprises dans les différentes bases de données créées par le projet, il est indiqué de prévoir dans le projet d'accord de coopération une disposition spécifique soumettant les personnes ayant accès à ces données au secret professionnel » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/002, SS. 10-11).

B.59. Laut den allgemeinen Erläuterungen des Zusammenarbeitsabkommens vom 25. August 2020 gehört die Unterwerfung der Mitarbeiter der Kontaktzentren unter das Berufsgeheimnis zu den Regeln für die Umsetzung der manuellen Kontaktrückverfolgung, die nicht in den Anwendungsbereich des Zusammenarbeitsabkommens fallen und die den Regelungen der föderierten Teilgebiete unterliegen:

« Les règles spécifiques relatives à la mise en œuvre du traçage (comme […] la soumission des travailleurs des centres de contact au secret professionnel) ne relèvent […] pas du champ

d'application de l'accord de coopération et sont régies par les réglementations applicables des autorités fédérées » (*Parl. Dok.*, Kammer, 2019-2020, DOC 55-1490/001, S. 64).

B.60. Wie die beklagten Behörden darlegen, unterliegen die Mitarbeiter des Kontaktzentrums bei der Wallonischen Agentur für Gesundheit, Sozialschutz, Behindertenwesen und Familie nach Artikel 5 des Sondervollmachtenerlasses Nr. 35 der Wallonischen Regierung vom 5. Mai 2020 « zur Organisation der Kontaktrückverfolgung im Rahmen der Bekämpfung der COVID-19-Epidemie » dem Berufsgeheimnis. Die Mitarbeiter des zentralen Kontaktzentrums, das bei der von der Flämischen Regierung benannten Struktur eingerichtet wurde, unterliegen nach Artikel 3 des Dekrets der Flämischen Gemeinschaft vom 29. Mai 2020 « zur Organisation der zentralisierten Kontaktermittlung durch einen Zusammenarbeitsverband externer Partner, der lokalen Kontaktermittlung durch die lokalen Verwaltungen oder die Fürsorgeräte und zur Organisation von COVID-19-Teams im Rahmen von COVID-19 » dem Berufsgeheimnis. Die Mitarbeiter des von der Regierung der Deutschsprachigen Gemeinschaft geschaffenen Kontaktzentrums unterliegen nach Artikel 10.18 § 2 des Dekrets der Deutschsprachigen Gemeinschaft vom 1. Juni 2004 « zur Gesundheitsförderung und zur medizinischen Prävention », eingefügt durch Artikel 18 des Dekrets vom 20. Juli 2020 « über die Rückverfolgung von Infektionsketten im Rahmen der Bekämpfung der Coronavirus (COVID-19) Gesundheitskrise », dem Berufsgeheimnis.

Artikel 4 § 2 des Sondervollmachtenerlasses Nr. 2020/006 des Vereinigten Kollegiums der Gemeinsamen Gemeinschaftskommission vom 18. Juni 2020 « zur Organisation der Kontaktrückverfolgung im Rahmen der Bekämpfung der COVID-19-Pandemie » untersagt es den Mitgliedern des bei den Diensten des Vereinigten Kollegiums der Gemeinsamen Gemeinschaftskommission organisierten Kontaktzentrums, personenbezogene Daten, zu denen sie Zugang haben, weiterzugeben oder zu einem anderen Zweck zu nutzen. Nach Artikel 13 desselben Erlasses kann ein Verstoß gegen dieses Verbot mit den in Artikel 15 der Ordonnanz der Gemeinsamen Gemeinschaftskommission vom 19. Juli 2007 « über die präventive Gesundheitspolitik » vorgesehenen strafrechtlichen Sanktionen belegt werden.

Daraus ergibt sich, dass die Mitarbeiter der Kontaktzentren alle einer gesetzlichen Geheimhaltungspflicht unterliegen, deren Missachtung strafrechtlich geahndet wird.

B.61. In der Auslegung, dass die Mitarbeiter der in Artikel 1 § 1 Nr. 4 des Zusammenarbeitsabkommens vom 25. August 2020 erwähnten Kontaktzentren, einschließlich der in Artikel 1 § 1 Nr. 20 erwähnten Felduntersucher, verpflichtet sind, die personenbezogenen Daten, von denen sie bei der Ausübung ihrer Aufträge Kenntnis erhalten, gemäß den in B.60 erwähnten Rechtsvorschriften geheim zu halten, verstößt das Zusammenarbeitsabkommen vom 25. August 2020 nicht gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten.

B.62. Vorbehaltlich der in B.61 erwähnten Auslegung ist der neunte Teil des einzigen Klagegrunds unbegründet.

In Bezug auf den Antrag, eine Vorabentscheidungsfrage beim Gerichtshof der Europäischen Union zu stellen

B.63. Die klagenden Parteien schlagen vor, dem Gerichtshof eine Vorabentscheidungsfragen zur Auslegung des Unionsrechts zu stellen.

Die Prüfung der Beschwerdegründe hat keine Zweifel in Bezug auf die Auslegung der im vorliegenden Fall anwendbaren Bestimmungen des Unionsrechts ergeben, sodass dem vorerwähnten Antrag nicht stattzugeben ist.

In Bezug auf den Antrag zur Aufrechterhaltung der Folgen

B.64. Die beklagten Behörden beantragen die Aufrechterhaltung der Folgen der angefochtenen Akte im Fall einer Nichtigerklärung.

B.65.1. Wenn eine gegen eine Gesetzesnorm gerichtete Nichtigkeitsklage begründet ist, hat der Gerichtshof gemäß Artikel 8 Absatz 1 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof (nachstehend: Sondergesetz) nur die Befugnis, den angefochtenen Akt vollständig oder teilweise für nichtig zu erklären.

Wenn er wie im vorliegenden Fall eine Gesetzesnorm aus dem Grund für nichtig erklärt, dass der Gesetzgeber es in verfassungswidriger Weise unterlassen hat, gesetzgeberisch aufzutreten, kann der Gerichtshof gemäß Artikel 8 Absatz 3 des Sondergesetzes die Wirkungen einer für nichtig erklärten Bestimmung für die von ihm festgelegte Frist vorläufig aufrechterhalten, bis der Gesetzgeber der festgestellten Verfassungswidrigkeit ein Ende gesetzt hat.

B.65.2. Aus der Rechtsprechung des Europäischen Gerichtshofes geht hervor, dass die Grundsätze des Vorrangs und der vollen Wirksamkeit des Rechts der Europäischen Union einer vorübergehenden Aufrechterhaltung einzelstaatlicher Maßnahmen, die gegen das unmittelbar geltende Recht der Union verstoßen, im Wege stehen (EuGH, Große Kammer, 8. September 2010, C-409/06, *Winner Wetten GmbH*). In Anbetracht dieser Rechtsprechung kann der Verfassungsgerichtshof folglich einem Antrag auf Aufrechterhaltung der Wirkungen eines für nichtig erklärten Gesetzgebungsaktes nicht stattgeben, da so die volle Wirksamkeit des Unionsrechts beeinträchtigt würde.

Wenn der Gerichtshof anhand der geprüften Klagegründe jedoch feststellt, dass eine Gesamtheit von gesetzgeberischen Maßnahmen mit der Verfassung in Verbindung mit der DSGVO im Einklang steht, mit Ausnahme von Lücken, die in der fehlenden Festlegung einer maximalen Aufbewahrungsfrist von in einer Datenbank gespeicherten personenbezogenen Daten und der fehlenden Benennung von einigen Einrichtungen als gemeinsam Verantwortliche der Datenverarbeitung bestehen, stellt der Gerichtshof die volle Wirksamkeit des Unionsrechts sicher, indem er dem Gesetzgeber eine kurze Frist auferlegt, in der dieser der festgestellten Verfassungswidrigkeit ein Ende setzen muss.

B.65.3. Zur Wahrung der Rechtssicherheit der auf der Grundlage des Zusammenarbeitsabkommens vom 25. August 2020 vorgenommenen Verarbeitung personenbezogener Daten sind die Folgen der angefochtenen Akte aufrechtzuerhalten, insoweit sie Folgendes billigen:

- die Artikel 2 § 3 und 15 §§ 1 und 3 zweiter Satz des Zusammenarbeitsabkommens vom 25. August 2020, bis die betreffenden Gesetzgeber ein ergänzendes Zusammenarbeitsabkommen billigen, in dem eine maximale Aufbewahrungsfrist der in der

Datenbank IV gespeicherten personenbezogenen Daten vorgesehen ist, und spätestens bis zum 31. März 2023;

- Artikel 2 § 4 desselben Zusammenarbeitsabkommens, bis die betreffenden Gesetzgeber ein ergänzendes Zusammenarbeitsabkommen billigen, das bestimmt, dass die zuständigen föderierten Teilgebiete oder ihre Agenturen, unter deren Aufsicht die Kontaktzentren, die mobilen Teams und die Gesundheitsinspektionsdienste arbeiten, gemeinsam Verantwortliche der Datenbank I sind, und spätestens bis zum 31. März 2023.

B.65.4. Im Übrigen ist in Anbetracht der begrenzten Tragweite der ausgesprochenen Nichtigerklärung diesem Antrag nicht stattzugeben.

Aus diesen Gründen:

Der Gerichtshof

1) erklärt das Dekret der Wallonischen Region vom 30. September 2020, Artikel 1 des Dekrets der Deutschsprachigen Gemeinschaft vom 12. Oktober 2020, Artikel 2 des Gesetzes vom 9. Oktober 2020, die Ordonnanz der Gemeinsamen Gemeinschaftskommission vom 1. Oktober 2020 und das Dekret der Flämischen Gemeinschaft vom 2. Oktober 2020 « zur Billigung 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, Gesundheitsinspektionsdienste und mobilen Teams im Rahmen einer Kontaktermittlung bei (vermutlich) mit dem Coronavirus COVID-19 infizierten Personen auf der Grundlage einer Datenbank bei Sciensano », insoweit sie Folgendes billigen:

- die Artikel 2 § 3 und 15 §§ 1 und 3 zweiter Satz des Zusammenarbeitsabkommens vom 25. August 2020, insofern diese Bestimmungen keine maximale Aufbewahrungsfrist der in der Datenbank IV gespeicherten personenbezogenen Daten vorsehen,

- Artikel 2 § 4 desselben Zusammenarbeitsabkommens, insofern diese Bestimmung nicht vorsieht, dass die zuständigen föderierten Teilgebiete oder ihre Agenturen, unter deren Aufsicht die Kontaktzentren, die mobilen Teams und die Gesundheitsinspektionsdienste arbeiten, gemeinsam Verantwortliche der Datenbank I sind,

- dasselbe Zusammenarbeitsabkommen, insofern sein Artikel 11 § 1 die Wörter « sowohl » und « als auch die weitere Mitteilung dieser personenbezogenen Daten von Sciensano an Dritte wie in Artikel 10 vorgesehen » enthält, und

- Artikel 10 § 3 zweiter Satz desselben Zusammenarbeitsabkommens

für nichtig;

2) weist die Klagen vorbehaltlich der in B.30.4 und B.61 erwähnten Auslegungen und unter Berücksichtigung des in B.55.2 Erwähnten im Übrigen zurück;

3) erhält die Folgen der für nichtig erklärten Akte aufrecht, insoweit sie Folgendes billigen:

- die Artikel 2 § 3 und 15 §§ 1 und 3 zweiter Satz des Zusammenarbeitsabkommens vom 25. August 2020, bis die betreffenden Gesetzgeber ein ergänzendes Zusammenarbeitsabkommen billigen, in dem eine maximale Aufbewahrungsfrist der in der Datenbank IV gespeicherten personenbezogenen Daten vorgesehen ist, und spätestens bis einschließlich 31. März 2023, und

- Artikel 2 § 4 desselben Zusammenarbeitsabkommens, bis die betreffenden Gesetzgeber ein ergänzendes Zusammenarbeitsabkommen billigen, das bestimmt, dass die zuständigen föderierten Teilgebiete oder ihre Agenturen, unter deren Aufsicht die Kontaktzentren, die mobilen Teams und die Gesundheitsinspektionsdienste arbeiten, gemeinsam Verantwortliche der Datenbank I sind, und spätestens bis einschließlich 31. März 2023.

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 22. September 2022.

Der Kanzler, Der Präsident,

P.-Y. Dutilleux P. Nihoul