



Verfassungsgerichtshof

Entscheid Nr. 84/2023
vom 1. Juni 2023
Geschäftsverzeichnisnr. 7648

In Sachen: Klage auf Nichtigerklärung des Gesetzes vom 2. April 2021, des Dekrets der Flämischen Gemeinschaft vom 2. April 2021, des Dekrets der Französischen Gemeinschaft vom 25. März 2021, des Dekrets der Deutschsprachigen Gemeinschaft vom 29. März 2021, der Ordonnanz der Gemeinsamen Gemeinschaftskommission vom 2. April 2021, des Dekrets der Wallonischen Region vom 1. April 2021 und des Dekrets der Französischen Gemeinschaftskommission vom 1. April 2021 « zur Billigung des Zusammenarbeitsabkommens vom 12. März 2021 zwischen dem Föderalstaat, der Flämischen Gemeinschaft, der Französischen Gemeinschaft, der Deutschsprachigen Gemeinschaft, der Gemeinsamen Gemeinschaftskommission, der Wallonischen Region und der Französischen Gemeinschaftskommission über die Verarbeitung von Daten im Zusammenhang mit Impfungen gegen COVID-19 », erhoben von Charlotte D'Hondt.

Der Verfassungsgerichtshof,

zusammengesetzt aus den Präsidenten P. Nihoul und L. Lavrysen, und den Richtern T. Giet, J. Moerman, M. Pâques, Y. Kherbache, T. Detienne, D. Pieters, S. de Bethune, E. Bribosia, W. Verrijdt und K. Jadin, unter Assistenz des Kanzlers F. Meersschant, unter dem Vorsitz des Präsidenten P. Nihoul,

erlässt nach Beratung folgenden Entscheid:

I. Gegenstand der Klage und Verfahren

Mit einer Klageschrift, die dem Gerichtshof mit am 7. Oktober 2021 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 8. Oktober 2021 in der Kanzlei eingegangen ist, erhob Charlotte D'Hondt, unterstützt und vertreten durch RA P. Joassart, in Brüssel zugelassen, Klage auf Nichtigerklärung des Gesetzes vom 2. April 2021, des Dekrets der Flämischen Gemeinschaft vom 2. April 2021, des Dekrets der Französischen Gemeinschaft vom 25. März 2021, des Dekrets der Deutschsprachigen Gemeinschaft vom 29. März 2021, der Ordonnanz der Gemeinsamen Gemeinschaftskommission vom 2. April 2021, des Dekrets der Wallonischen Region vom 1. April 2021 und des Dekrets der Französischen Gemeinschaftskommission vom 1. April 2021 « zur Billigung des Zusammenarbeitsabkommens vom 12. März 2021 zwischen dem Föderalstaat, der Flämischen Gemeinschaft, der Französischen Gemeinschaft, der Deutschsprachigen Gemeinschaft, der

Gemeinsamen Gemeinschaftskommission, der Wallonischen Region und der Französischen Gemeinschaftskommission über die Verarbeitung von Daten im Zusammenhang mit Impfungen gegen COVID-19 » (jeweils veröffentlicht im *Belgischen Staatsblatt* vom 12. April 2021, zweite Ausgabe, vom 9. April 2021, vom 6. April 2021, vom 12. April 2021, zweite Ausgabe, vom 9. April 2021, vom 12. April 2021, zweite Ausgabe, und vom 7. April 2021).

Schriftsätze und Gegenerwiderungsschriftsätze wurden eingereicht von

- dem Ministerrat, unterstützt und vertreten durch RA P. Slegers, RÄin S. Ben Messaoud und RÄin J. Duval, in Brüssel zugelassen,

- der Flämischen Regierung, der Wallonischen Regierung, dem Kollegium der Französischen Gemeinschaftskommission, dem Vereinigten Kollegium der Gemeinsamen Gemeinschaftskommission, der Regierung der Französischen Gemeinschaft und der Regierung der Deutschsprachigen Gemeinschaft, unterstützt und vertreten durch RÄin M. Feys, in Gent zugelassen.

Die klagende Partei hat einen Erwiderungsschriftsatz eingereicht.

Durch Anordnung vom 15. März 2023 hat der Gerichtshof nach Anhörung der referierenden Richter T. Giet und S. de Bethune beschlossen, dass die Rechtssache verhandlungsreif ist, dass keine Sitzung abgehalten wird, außer wenn eine Partei innerhalb von sieben Tagen nach Erhalt der Notifizierung dieser Anordnung einen Antrag auf Anhörung eingereicht hat, und dass vorbehaltlich eines solchen Antrags die Verhandlung am 29. März 2023 geschlossen und die Rechtssache zur Beratung gestellt wird.

Da keine Sitzung beantragt wurde, wurden die Rechtssachen am 29. März 2023 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 die angefochtenen Akte und ihren Kontext

B.1. Die klagende Partei beantragt die Nichtigkeitsklärung des Gesetzes vom 2. April 2021, des Dekrets der Flämischen Gemeinschaft vom 2. April 2021, des Dekrets der Französischen Gemeinschaft vom 25. März 2021, des Dekrets der Deutschsprachigen Gemeinschaft vom 29. März 2021, der Ordonnanz der Gemeinsamen Gemeinschaftskommission vom 2. April

2021, des Dekrets der Wallonischen Region vom 1. April 2021 und des Dekrets der Französischen Gemeinschaftskommission vom 1. April 2021 «zur Billigung des Zusammenarbeitsabkommens vom 12. März 2021 zwischen dem Föderalstaat, der Flämischen Gemeinschaft, der Französischen Gemeinschaft, der Deutschsprachigen Gemeinschaft, der Gemeinsamen Gemeinschaftskommission, der Wallonischen Region und der Französischen Gemeinschaftskommission über die Verarbeitung von Daten im Zusammenhang mit Impfungen gegen COVID-19 » (nachstehend: Zusammenarbeitsabkommen vom 12. März 2021).

Das Zusammenarbeitsabkommen vom 12. März 2021 wurde in den drei Landessprachen in der Anlage zum Gesetz vom 2. April 2021 im *Belgischen Staatsblatt* vom 12. April 2021 veröffentlicht.

B.2.1. Am 11. März 2020 stufte die Weltgesundheitsorganisation den Ausbruch des Coronavirus SARS-CoV-2 als Pandemie ein. Auch Belgien ist seit März 2020 mit dieser Pandemie und ihren Folgen konfrontiert. Das Coronavirus SARS-CoV-2 ist ein sehr ansteckendes Virus, das die Krankheit COVID-19 hervorruft, die hauptsächlich bei älteren Personen und Personen mit einer Krankengeschichte ernsthafte medizinische Probleme verursacht oder tödlich enden kann (*Parl. Dok.*, Flämisches Parlament, 2019-2020, Nr. 415/1, S. 2; *Parl. Dok.*, Flämisches Parlament, 2020-2021, Nr. 488/1, S. 2; *Parl. Dok.*, Vereinigte Versammlung der Gemeinsamen Gemeinschaftskommission, 2019-2020, Nr. B-41/1, S. 1).

Im Rahmen dieser COVID-19-Gesundheitskrise und zur Verhinderung der weiteren Ausbreitung der Krankheit COVID-19 wurde ursprünglich der Nationale Sicherheitsrat und danach der Konzertierungsausschuss, in den Vertreter der Föderalbehörde und der Gliedstaaten berufen wurden, damit beauftragt, aufeinander abgestimmte Maßnahmen zu ergreifen, um die weitere Verbreitung von COVID-19 zu begrenzen (*Parl. Dok.*, Flämisches Parlament, 2019-2020, Nr. 415/1, S. 2; *Parl. Dok.*, Flämisches Parlament, 2020-2021, Nr. 488/1, S. 2).

B.2.2. Die angefochtenen Akte stehen im Zusammenhang mit der Ergänzung und der Aktualisierung des Arsenal an Maßnahmen, die die verschiedenen Behörden ergriffen haben, um die COVID-19-Pandemie zu bekämpfen und die weitere Verbreitung des Coronavirus SARS-CoV-2 zu verhindern, sowie um ein Wiederaufflammen der COVID-19-Pandemie zu

vermeiden. Die angefochtenen Akte stehen insbesondere mit den für die Organisation der Impfung gegen COVID-19 notwendigen Maßnahmen im Zusammenhang.

Wie in anderen Ländern, die an dem europäischen Verfahren zur Beschaffung von COVID-19-Impfstoffen teilnehmen, in dem die Europäische Kommission im Namen der Mitgliedstaaten mit den Unternehmen nach der Marktzulassung und entsprechend der Produktionskapazitäten verhandelt, haben der Föderalstaat und die föderierten Teilgebiete entschieden zusammenzuarbeiten, um eine freiwillige und kostenlose Massenimpfkampagne gegen COVID-19 zu organisieren.

Diese Entscheidung stützte sich insbesondere auf Studien, die die klinische Wirksamkeit der breit angelegten Impfung gegen das sehr ansteckende Coronavirus SARS-CoV-2, das die Krankheit COVID-19 verursacht, zeigten, um die Ausbreitung von Ansteckungen mit dieser Krankheit zu bekämpfen und eine Überlastung der Krankenhäuser wegen der sich daraus ergebenden Krankenhauseinweisungen zu vermeiden sowie um ein Wiederaufflammen der COVID-19-Pandemie zu verhindern. Die Weltgesundheitsorganisation empfiehlt der Öffentlichkeit ebenfalls, sich gegen COVID-19 impfen zu lassen.

Die Interministerielle Konferenz Volksgesundheit vom 16. November 2020 hat die wesentlichen Grundsätze definiert, die der belgischen Strategie der Impfung gegen COVID-19 zugrunde liegen:

- Ziel einer Impfabdeckung von 70 % der Bevölkerung;
- Festlegung der prioritären Gruppen auf der Grundlage wissenschaftlicher Gutachten;
- Kostenlose Impfung auf freiwilliger Basis für jeden Bürger;
- Kofinanzierung des gesamten Impfprogramms durch den Föderalstaat und die föderierten Teilgebiete.

Diese Entscheidungen hängen von folgenden Elementen ab:

- Massenimpfkampagnen, da die Impfstoffe in Mehrfachdosis-Fläschchen geliefert werden, die am selben Tag verabreicht werden müssen;
- Bereitstellung von einem oder mehreren wirksamen und sicheren Impfstoffen gegen COVID-19 in Belgien;

- Fähigkeit des belgischen Gesundheitssystems zur Verteilung und schrittweisen und effektiven Impfung der Bevölkerung, wobei die Gesundheitsbehörden durch die interföderale Task Force « COVID-19-Impfstoff », die von der Interministeriellen Konferenz Volksgesundheit am 16. November 2020 gegründet wurde, durch sämtliche Gesundheitsstrukturen des Landes, darunter Sciensano, und die Föderalagentur für Arzneimittel und Gesundheitsprodukte (FAAGP) unterstützt werden. Die Registrierungssoftware Vaccinnet+ wird von allen förderierten Teilgebieten zu diesem Zweck verwendet;

- Bestreben, durch Überzeugungsarbeit und Transparenz die Impfskepsis zu überwinden und so die Akzeptanz der Bevölkerung für diese Gesundheitsstrategie zu erhalten.

Die Impfstrategie gegen COVID-19 wurde in mehreren Phasen ab dem Monat Januar 2021 mit einer Priorisierung der Zielgruppen umgesetzt, wobei die prioritären Gruppen die Altenheimbewohner und ein Teil der Personalmitglieder der Altenheime, das Krankenhauspersonal und das Pflege- und Hilfspersonal, das an vorderster Front arbeitet, waren. Ab Februar 2021 wurden die prioritären Gruppen auf Risikopersonen mit Begleiterkrankungen, auf Personen im Alter von 65 Jahren und darüber und auf Personen im Alter von 18 bis 55 Jahren bei den Polizeikräften ausgedehnt, bevor sie schrittweise auf der Grundlage des Kriteriums des Alters und der Schutzbedürftigkeit auf die gesamte Bevölkerung über 18 Jahren, sodann über 16 Jahren, über 12 Jahren und schließlich ab 5 Jahren erweitert wurden.

Auf der Grundlage des aktualisierten wissenschaftlichen Kenntnisstandes wurde von der interföderalen Task Force « COVID-19-Impfstoff » ein Impfschema mit einer oder zwei Impfstoffdosen je nach dem verabreichten Impfstoff erstellt und die Möglichkeit, eine « Boosterdosis » zu erhalten, wurde der Bevölkerung ebenfalls angeboten.

B.2.3.1. Diese Massenimpfkampagne hängt ebenfalls eng mit den neuen, im Juli 2020 ergriffenen Maßnahmen zusammen, um die Risiken einer Ausbreitung im Zusammenhang mit den Lockerungen der Einschränkungen von physischen Kontakten und der Möglichkeit, wieder zu reisen, in Anbetracht der neuen Phase der COVID-19-Krise zu bekämpfen.

B.2.3.2. Die Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates vom 14. Juni 2021 « über einen Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von COVID-19-Impfungen und -Tests sowie der Genesung von einer COVID-19-Infektion (digitales COVID-Zertifikat der EU) mit der

Zielsetzung der Erleichterung der Freizügigkeit während der COVID-19-Pandemie » (nachstehend: der Verordnung (EU) 2021/953) legt nach ihrem Artikel 1 Absatz 1 einen Rahmen für die Ausstellung, Überprüfung und Anerkennung des digitalen EU-COVID-Zertifikats, das heißt eines interoperables, im Kontext der COVID-19-Pandemie ausgestellten Zertifikats mit Informationen über Impfungen, Testergebnisse sowie die Genesung des Zertifikationsinhabers, mit der Zielsetzung fest, den Inhabern die Ausübung ihres Rechts auf Freizügigkeit während der COVID-19-Pandemie zu erleichtern.

Das digitale EU-COVID-Zertifikat ermöglicht die Ausstellung, grenzüberschreitende Überprüfung und Anerkennung insbesondere eines Impfbzertifikats, das bestätigt, dass der Inhaber in dem Mitgliedstaat, der das Zertifikat ausstellt, einen Impfstoff gegen COVID-19 erhalten hat.

Die Erwägungsgründe 8 und 29 der Verordnung (EU) 2021/953 lauten:

«(8) Viele Mitgliedstaaten haben Initiativen zur Ausstellung von COVID-19-Impfbzertifikaten eingeleitet oder verfolgen entsprechende Pläne. Diese Impfbzertifikate müssen allerdings vollständig interoperabel, kompatibel, sicher und überprüfbar sein, damit sie in einem grenzüberschreitenden Kontext, wenn Unionsbürger ihr Recht auf Freizügigkeit ausüben, wirksam verwendet werden können. Inhalt, Format, Grundsätze, technische Standards und die Sicherheitsstufe solcher Impfbzertifikate bedürfen eines gemeinsamen Konzepts der Mitgliedstaaten.

[...]

(29) Zwecks Erleichterung der Freizügigkeit und um sicherzustellen, dass die aktuellen Beschränkungen der Freizügigkeit während der COVID-19-Pandemie auf koordinierte Weise auf Grundlage der aktuellsten wissenschaftlichen Erkenntnisse und der von dem mit Artikel 17 des Beschlusses Nr. 1082/2013/EU des Europäischen Parlaments und des Rates eingesetzten Gesundheitssicherheitsausschuss, dem ECDC und der Europäischen Arzneimittel-Agentur (EMA) bereitgestellten Leitlinien aufgehoben werden können, sollte ein interoperables Impfbzertifikat festgelegt werden. Mit diesem Impfbzertifikat sollte bestätigt werden, dass der Inhaber in einem Mitgliedstaat einen COVID-19-Impfstoff erhalten hat, und es sollte dazu beitragen, die Beschränkungen der Freizügigkeit schrittweise aufzuheben. Das Impfbzertifikat sollte lediglich die Informationen enthalten, die erforderlich sind, um den Inhaber sowie den verabreichten COVID-19-Impfstoff, die Anzahl der Dosen und das Datum sowie den Ort der Impfung eindeutig identifizieren zu können. Die Mitgliedstaaten sollten Impfbzertifikate für Personen ausstellen, die COVID-19-Impfstoffe erhalten haben, deren Inverkehrbringen gemäß der Verordnung (EG) Nr. 726/2004 des Europäischen Parlaments und des Rates genehmigt wurde, für Personen, die COVID-19-Impfstoffe erhalten haben, für die eine Genehmigung für das Inverkehrbringen von der zuständigen Behörde eines Mitgliedstaats gemäß der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates erteilt wurde, und für

Personen, die COVID-19-Impfstoffe erhalten haben, deren Inverkehrbringen gemäß Artikel 5 Absatz 2 der genannten Richtlinie vorübergehend gestattet wurde ».

Artikel 5 der Verordnung (EU) 2021/953 mit der Überschrift « Impfbzertifikat » bestimmt:

« (1) Jeder Mitgliedstaat stellt Personen, denen ein COVID-19-Impfstoff verabreicht wurde, entweder automatisch oder auf Antrag dieser Personen Impfbzertifikate nach Artikel 3 Absatz 1 Buchstabe a aus. Die betreffenden Personen werden über ihr Recht auf Ausstellung eines Impfbzertifikats unterrichtet.

(2) Das Impfbzertifikat enthält folgende Kategorien personenbezogener Daten:

- a) Identität des Inhabers;
- b) Informationen über den COVID-19-Impfstoff und die die dem Inhaber verabreichten Anzahl der Dosen;
- c) Zertifikatmetadaten, z. B. Zertifikataussteller oder eine eindeutige Zertifikatkennung.

Die personenbezogenen Daten werden in das Impfbzertifikat gemäß den spezifischen Datenfeldern nach Nummer 1 des Anhangs aufgenommen.

Der Kommission wird die Befugnis übertragen, gemäß Artikel 12 delegierte Rechtsakte zu erlassen, um Nummer 1 des Anhangs durch Änderung oder Streichung von Datenfeldern oder durch Hinzufügung von Datenfeldern, die unter die unter die in Unterabsatz 1 Buchstaben b und c dieses Absatzes genannten Kategorien personenbezogener Daten fallen, zu ändern, wenn eine solche Änderung erforderlich ist, um die Echtheit, Gültigkeit und Integrität des Impfbzertifikats zu überprüfen und zu bestätigen, wenn wissenschaftliche Fortschritte hinsichtlich der Eindämmung der COVID-19-Pandemie erzielt wurden, oder um die Interoperabilität mit internationalen Standards sicherzustellen.

(3) Das Impfbzertifikat wird nach der Verabreichung jeder einzelnen Dosis in einem sicheren und interoperablen Format nach Artikel 3 Absatz 2 ausgestellt, und daraus geht eindeutig hervor, ob das Impfprogramm abgeschlossen wurde oder nicht.

(4) Wenn angesichts neuer wissenschaftlicher Erkenntnisse oder zwecks Gewährleistung der Interoperabilität mit internationalen Standards und technologischen Systemen Gründe äußerster Dringlichkeit es zwingend erforderlich machen, findet das in Artikel 13 genannte Verfahren auf die gemäß dem vorliegenden Artikel erlassenen delegierten Rechtsakte Anwendung.

(5) Wenn Mitgliedstaaten Impfnachweise anerkennen, um im Einklang mit dem Unionsrecht eingeführte Beschränkungen der Freizügigkeit zur Eindämmung der Ausbreitung von SARS-CoV-2 aufzuheben, erkennen sie unter denselben Bedingungen auch gültige Impfbzertifikate an, die von anderen Mitgliedstaaten im Einklang mit dieser Verordnung für einen COVID-19-Impfstoff ausgestellt wurden, dessen Inverkehrbringen gemäß der Verordnung (EG) Nr. 726/2004 genehmigt wurde.

Die Mitgliedstaaten können zu demselben Zweck Impfbzertifikate anerkennen, die von anderen Mitgliedstaaten gemäß dieser Verordnung für einen COVID-19-Impfstoff, für dessen Inverkehrbringen die zuständige Behörde eines Mitgliedstaats nach der Richtlinie 2001/83/EG eine Genehmigung erteilt hat, einen COVID-19-Impfstoff, dessen Inverkehrbringen nach Artikel 5 Absatz 2 der genannten Richtlinie vorübergehend gestattet wurde, oder einen COVID-19-Impfstoff, der das Verfahren der Notfallzulassung der WHO durchlaufen hat, ausgestellt wurden.

Erkennen die Mitgliedstaaten Impfbzertifikate für einen in Unterabsatz 2 genannten COVID-19-Impfstoff an, so erkennen sie zu gleichen Bedingungen auch Impfbzertifikate an, die von anderen Mitgliedstaaten gemäß der vorliegenden Verordnung für den selben COVID-19-Impfstoff ausgestellt wurden ».

Der Anhang mit der Überschrift « In den Zertifikaten enthaltene Datensätze » sieht in Nummer 1 vor:

« In das Impfbzertifikat aufzunehmende Datenfelder:

- a) Name: Nachname(n) und Vorname(n) (in dieser Reihenfolge);
- b) Geburtsdatum;
- c) Zielkrankheit oder -erreger: COVID-19 (SARS-CoV-2 oder eine seiner Varianten);
- d) COVID-19-Impfstoff oder -Prophylaxe;
- e) COVID-19-Impfstoffhandelsname;
- f) Zulassungsinhaber oder Hersteller des COVID-19-Impfstoffs;
- g) Nummer der Impfung in einer Impfsrie und Gesamtzahl der Dosen in der Impfsrie;
- h) Datum der Impfung (unter Angabe des Datums der letzten Wiederimpfung);
- i) Mitgliedstaat oder Drittland, in dem der Impfstoff verabreicht wurde;
- j) Zertifikataussteller;
- k) eindeutige Zertifikatkennung ».

B.2.3.3. In den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 11. Juni 2021 zwischen dem Föderalstaat, der Flämischen Gemeinschaft, der Französischen Gemeinschaft, der Deutschsprachigen Gemeinschaft, der Gemeinsamen Gemeinschaftskommission, der Wallonischen Region und der Französischen Gemeinschaftskommission in Bezug auf die operative Umsetzung der Verordnung (EU) des

Europäischen Parlaments und des Rates über einen Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von Impfungen, Tests und der Genesung mit der Zielsetzung der Erleichterung der Freizügigkeit während der COVID-19-Pandemie (Digitales EU-COVID-Zertifikat) heißt es:

« Im Zusammenarbeitsabkommen vom 12. März 2021 zwischen dem Föderalstaat, der Flämischen Gemeinschaft, der Französischen Gemeinschaft, der Deutschsprachigen Gemeinschaft, der Gemeinsamen Gemeinschaftskommission, der Wallonischen Region und der Französischen Gemeinschaftskommission über die Verarbeitung von Daten im Zusammenhang mit Impfungen gegen COVID-19 [...] wird das gemeinsame Informationssystem festgelegt, das zur Einladung, Organisation und Registrierung im Hinblick auf die Impfung von Personen dient. Die föderierten Teilgebiete und die Föderalbehörde sehen die Einrichtung eines solchen Systems als eine entscheidende Voraussetzung für die Bewältigung der aktuellen Krise an. Um die Einladung von zu impfenden Personen und die Organisation der Impfung zu unterstützen, wurde ein gemeinsames Informationssystem benötigt, um unkoordinierte Einladungen von Personen oder doppelte Einladungen von bereits geimpften Personen zu vermeiden. Darüber hinaus muss das System die Bestimmung des geeigneten Dosierungsschemas ermöglichen, einschließlich der verschiedenen zu verabreichenden Dosen eines Impfstoffs (korrektes Intervall im Falle eines Mehrfachdosis-Impfstoffs), und sicherstellen, dass die Impfung je nach Verfügbarkeit der erforderlichen Ausrüstung und des (medizinischen) Personals ordnungsgemäß organisiert wird. Die Registrierung von Impfungen in einem gemeinsamen Informationssystem (Vaccinnet) durch flämische, Brüsseler, wallonische und deutschsprachige Impfberechtigte war unter anderem notwendig. Die Datenbank wird in sehr enger Zusammenarbeit zwischen den föderierten Teilgebieten und dem Föderalstaat entwickelt und verwaltet. Daher ist es angebracht, auch für die Ausstellung der Zertifikate dasselbe Betriebssystem zu benutzen » (*Belgisches Staatsblatt* vom 14. Juni 2021, zweite Ausgabe, S. 61955).

B.2.3.4. Die Zusammenarbeitsabkommen vom 14. Juli 2021 und 27. September 2021 zwischen dem Föderalstaat, der Flämischen Gemeinschaft, der Französischen Gemeinschaft, der Deutschsprachigen Gemeinschaft, der Gemeinsamen Gemeinschaftskommission, der Wallonischen Region und der Französischen Gemeinschaftskommission über die Verarbeitung von Daten im Zusammenhang mit dem digitalen EU-COVID-Zertifikat, dem COVID Safe Ticket, dem PLF und der Verarbeitung personenbezogener Daten von Lohnempfängern und Selbständigen, die im Ausland leben oder wohnen und in Belgien Tätigkeiten ausüben, sowie das Zusammenarbeitsabkommen vom 28. Oktober 2021, das dasjenige vom 14. Juli 2021 abändert, legen eine Rechtsgrundlage für die landesweite Verwendung des digitalen EU-COVID-Zertifikats und die Erstellung des COVID Safe Tickets (nachstehend: CST) auf der Grundlage des digitalen EU-COVID-Zertifikats fest. Die Impfung einer Person gegen COVID-19 ermöglicht es, das CST automatisch zu generieren.

In den allgemeinen Erläuterungen zu dem vorerwähnten Zusammenarbeitsabkommen vom 14. Juli 2021 heißt es diesbezüglich, dass nach dem zum Zeitpunkt der Annahme des Abkommens verfügbaren wissenschaftlichen Kenntnisstand geimpfte Personen ein geringeres Risiko aufweisen, andere mit dem Coronavirus SARS-CoV-2 zu infizieren (*Belgisches Staatsblatt* vom 23. Juli 2021, S. 76172; siehe auch Erwägungsgrund 7 der Verordnung (EU) 2021/953).

Artikel 11 des Zusammenarbeitsabkommens vom 14. Juli 2021 bestimmt:

« § 1. Zum Zweck der Überprüfung und zur Erstellung und Ausstellung des digitalen EU-COVID-Zertifikats für Inhaber eines Impfzertifikats, Testzertifikats oder Genesungszertifikats werden folgende Kategorien personenbezogener Daten verarbeitet:

1. die in Artikel 9 §§ 1, 2 und 3 erwähnten Kategorien personenbezogener Daten,
2. die in Artikel 8 des Gesetzes vom 15. Januar 1990 über die Errichtung und Organisation einer Zentralen Datenbank der sozialen Sicherheit erwähnte Erkennungsnummer und
3. der in Artikel 3 Absatz 1 Nr. 5 des Gesetzes vom 8. August 1983 zur Organisation eines Nationalregisters der natürlichen Personen in Belgien erwähnte Hauptwohnort.

§ 2. Die in § 1 erwähnten Kategorien personenbezogener Daten werden aus folgenden Datenbanken bezogen:

[...]

2. Vaccinnet: in Bezug auf die in Artikel 8 des Gesetzes vom 15. Januar 1990 über die Errichtung und Organisation einer Zentralen Datenbank der sozialen Sicherheit erwähnte Erkennungsnummer und die in Artikel 9 § 1 beschriebenen Kategorien personenbezogener Daten im Impfzertifikat,

[...]

§ 4. In Abweichung von Artikel 3 § 1 des Zusammenarbeitsabkommens vom 25. August 2020 und von Artikels 4 § 2 des Zusammenarbeitsabkommens vom 12. März 2021 dürfen die in § 1 erwähnten personenbezogenen Daten für die in Artikel 10 erwähnten Verarbeitungszwecke von den für die Verarbeitung Verantwortlichen für die Erfüllung ihrer im vorliegenden Zusammenarbeitsabkommen bestimmten gesetzlichen Aufträge, von den föderierten Teilgebieten und von Sciensano verarbeitet werden ».

B.3.1. Mit dem Zusammenarbeitsabkommen vom 12. März 2021 haben der Föderalstaat und die föderierten Teilgebiete « ein gemeinsames Informationssystem [...] zur Einladung, Organisation und Registrierung im Hinblick auf die Impfung von Personen » festgelegt (*Belgisches Staatsblatt* vom 12. April 2021, zweite Ausgabe, S. 32397):

«Die Registrierung von Impfungen in einem gemeinsamen Informationssystem (Vaccinnet) durch flämische, Brüsseler, wallonische und deutschsprachige Impfberechtigte ist unter anderem notwendig, um ein optimales Krisenmanagement zu betreiben, die Pharmakovigilanz gemäß Artikel 4 Nr. 2 des vorliegenden Abkommens zu ermöglichen, die Durchimpfungsrate der Bevölkerung zu überwachen und die Auswirkungen auf die Krankenversicherung zu erfassen.

Eine solche Registrierungspflicht erfordert angesichts der Tatsache, dass es sich um eine Notwendigkeit handelt und dass sie die Verarbeitung personenbezogener Daten beinhaltet, eine solide Rechtsgrundlage.

Die Datenbank wird in sehr enger Zusammenarbeit zwischen den föderierten Teilgebieten und dem Föderalstaat entwickelt und verwaltet » (ebenda, SS. 32397-32398).

B.3.2. In diesem Kontext sind im Zusammenarbeitsabkommen vom 12. März 2021 zwei verschiedene Datenbanken geregelt.

Einerseits wird, «um die Massenimpfkampagne im Rahmen der COVID-19-Pandemie gewährleisten zu können, [...] eine erste Impfcode-Datenbank entwickelt, durch die die Einladung der zu impfenden Personen, die Bestimmung des geeigneten Dosierungsschemas und die ordnungsgemäße Organisation der Impfung entsprechend der Verfügbarkeit der Impfstoffe und des Materials sowie des dafür erforderlichen Personals (medizinisches Personal und Krankenpflegepersonal) ermöglicht wird » (ebenda, S. 32398).

Diese Datenbank generiert einen zufälligen Impfcode für die gesamte Bevölkerung, die *a priori* geimpft werden kann, und erfasst die Daten zu diesen Personen, um das Impfschema gegen COVID-19 zu koordinieren und es zu vermeiden, dass ein neuer Impfcode für eine bereits geimpfte Person generiert wird (Artikel 2 § 1). Die in dieser Datenbank gespeicherten Daten werden durch Artikel 3 § 1 des Zusammenarbeitsabkommens vom 12. März 2021 festgelegt. Sie werden bis fünf Tage, gerechnet ab dem Tag nach dem Tag der Veröffentlichung des königlichen Erlasses zur Erklärung der Beendigung des Zustands der Epidemie des Coronavirus SARS-CoV-2, aufbewahrt (Artikel 6 § 1).

Auf der anderen Seite betrifft eine zweite Datenbank, « Vaccinnet », die Registrierung der Impfdaten der Personen, die sich impfen lassen, als solche durch die Person, die den Impfstoff gegen COVID-19 verabreicht hat, oder ihren Bevollmächtigten für das ganze Land (Artikel 2 § 2). Die Impfdaten sind in Artikel 3 § 2 des Zusammenarbeitsabkommens vom 12. März 2021

festgelegt als (1) Angaben zur Identität der Person, der die Impfung verabreicht worden ist, (2) Angaben zur Identität der Person, die die Impfung verabreicht hat, und gegebenenfalls ihre Kontaktdaten; (3) Daten, die sich auf den Impfstoff beziehen; (4) Datum und Ort der Verabreichung jeder Impfstoffdosis; (5) Daten über das Impfschema der Person gegen COVID-19, der der Impfstoff verabreicht wird; (6) gegebenenfalls Daten über unerwünschte Wirkungen, die während oder nach der Impfung bei der betreffenden Person beobachtet wurden und von denen die Person, die den Impfstoff verabreicht hat, oder ihr Bevollmächtigter Kenntnis hat. Diese Daten werden bis zum Tod der Person, der der Impfstoff gegen COVID-19 verabreicht wurde, und mindestens dreißig Jahre ab der Impfung aufbewahrt (Artikel 6 § 2).

Mit der Datenbank « Vaccinnet » werden « verschiedene Ziele in Zusammenhang mit der Impfung verfolgt: qualitativ hochwertige Gesundheitspflegeleistungen, Pharmakovigilanz, Rückverfolgbarkeit von Impfstoffen, Verwaltung der Impfschemas, logistische Organisation der Impfung, Ermittlung der Durchimpfungsrate, Organisation der Kontaktermittlung, Durchführung der Überwachung und Kontrolle, Berechnung der Aufteilung der Impfkosten und Durchführung wissenschaftlicher oder statistischer Studien » (ebenda, S.32400).

Die Verarbeitungszwecke der in den beiden Datenbanken erfassten Daten sind in Artikel 4 des Zusammenarbeitsabkommens vom 12. März 2021 aufgeführt. Die in diesen beiden Datenbanken erfassten Daten « dürfen nicht an Dritte übermittelt werden, es sei denn, durch Gesetz, Dekret oder Ordonnanz wird einem Dritten die Erlaubnis erteilt, Zugang zu diesen Daten zu erhalten oder sie ausschließlich zu den in Artikel 4 des Zusammenarbeitsabkommens erwähnten Zwecken in Zusammenhang mit der Impfung zu empfangen » (ebenda, S. 32401), nach Erlaubnis durch den Informationssicherheitsausschuss.

Für die beiden Datenbanken handeln die zuständigen föderierten Teilgebiete oder die von den zuständigen föderierten Teilgebieten bestimmten Agenturen und die Föderalbehörde jeweils in ihrem Zuständigkeitsbereich als Verantwortliche für die Verarbeitung der Daten (Artikel 7 § 1). Für Personen, die in den Zuständigkeitsbereich der Föderalbehörde fallen, ist Sciensano als Verantwortlicher für die Verarbeitung der Daten angegeben (Artikel 7 § 1 Nr. 7). Eine zentrale Anlaufstelle pro Gebiet und ein elektronisches Zugriffsrecht sind vorgesehen (Artikel 7 § 2).

Die Umsetzung und die Einhaltung des Zusammenarbeitsabkommens vom 12. März 2021 werden von der Interministeriellen Konferenz Volksgesundheit überwacht (Artikel 9 § 1).

B.4.1. Die Bestimmungen des Zusammenarbeitsabkommens vom 12. März 2021 entsprechen im Wesentlichen den Bestimmungen des königlichen Erlasses vom 24. Dezember 2020 « über die Registrierung und Verarbeitung von Daten über Impfungen gegen COVID-19 » (nachstehend: königlicher Erlass vom 24. Dezember 2020), gegen den die klagende Partei ebenfalls eine Nichtigkeitsklage vor dem Staatsrat erhoben hat. In der Präambel dieses königlichen Erlasses war angegeben, dass « es für die Volksgesundheit und zur Vermeidung eines Wiederaufflammens der COVID-19-Pandemie von entscheidender Bedeutung ist, dass die im Bereich der Impfungen notwendigen Maßnahmen ergriffen werden können » (*Belgisches Staatsblatt* vom 24. Dezember 2020, zweite Ausgabe, S. 94404), bis zum Abschluss eines Zusammenarbeitsabkommens.

Dieser königliche Erlass ist am 24. Dezember 2020, dem Datum seiner Veröffentlichung im *Belgischen Staatsblatt*, in Kraft getreten.

Artikel 9 des königlicher Erlasses vom 24. Dezember 2020 bestimmte:

« Le présent arrêté entre en vigueur au jour de sa publication dans le *Moniteur belge* et cesse ses effets le jour où entre en vigueur un accord de coopération entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant l'enregistrement et le traitement de données relatives aux vaccinations contre la COVID-19 ».

B.4.2.1. Der königliche Erlass vom 24. Dezember 2020 erging gemäß Artikel 11 des Gesetzes vom 22. Dezember 2020 « über verschiedene Maßnahmen in Bezug auf Antigen-Schnelltests und die Registrierung und Verarbeitung von Impfdaten im Rahmen der Bekämpfung der COVID-19-Pandemie » (nachstehend: Gesetz vom 22. Dezember 2020), der bestimmte:

« Ärzte oder Krankenpfleger, die den COVID-19-Impfstoff verabreichen oder die Impfung beaufsichtigen, registrieren jede Impfung in der von der Interministeriellen Konferenz Volksgesundheit bestimmten Datenbank. Der König legt durch einen im Ministerrat beratenen Erlass die Modalitäten dieser Registrierung fest und bestimmt zumindest die Zwecke der Datenverarbeitung, die Personenkategorien, für die die Daten verarbeitet werden, die

Kategorien der verarbeiteten Daten, die für die Verarbeitung Verantwortlichen und die Dauer der Aufbewahrung der Daten ».

B.4.2.2. In den Vorarbeiten zum Gesetz vom 22. Dezember 2020 wurde diesbezüglich dargelegt:

« L'article 11 impose l'obligation d'enregistrer chaque vaccination contre la COVID-19. Seuls les médecins ou les infirmiers sont légalement habilités à administrer des vaccins. La vaccination et l'enregistrement de la vaccination peuvent néanmoins être effectués par d'autres personnes sous leur supervision.

L'enregistrement des vaccinations est nécessaire pour mener une gestion de crise réfléchie, garantir le suivi médical (vigilance) de la personne vaccinée, suivre l'immunisation de la population et estimer l'impact sur l'assurance maladie et sur le nombre d'hospitalisations attendues.

L'enregistrement d'une vaccination implique le stockage dans une banque de données de données relatives à la personne vaccinée, de données relatives à la personne qui administre le vaccin, de données relatives aux circonstances d'administration du vaccin et de données relatives aux éventuels effets indésirables du vaccin.

La base de données sera créée et gérée en collaboration très étroite avec les entités fédérées. La Conférence interministérielle Santé publique désignera à cette fin la base de données dans laquelle les données visées seront sauvegardées.

Le Roi est habilité à fixer les conditions et les modalités s'appliquant à cet enregistrement, avec une attention particulière pour les aspects relatifs à la protection de la vie privée.

Il va toutefois sans dire que les données à caractère personnel collectées et traitées dans le cadre de cet enregistrement, seront traitées conformément à la réglementation relative à la protection à l'égard du traitement de données à caractère personnel, en particulier le Règlement général sur la protection des données, la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth.

Les entités fédérées et l'entité fédérale ont l'intention de préciser les règles de l'enregistrement et du traitement de données que celui-ci implique dans un Accord de coopération au sens de l'article 92*bis* de la loi spéciale de réformes institutionnelles du 8 août 1980. Vu l'extrême urgence d'entamer la vaccination et l'absolue nécessité d'enregistrer les vaccinations pour les raisons susmentionnées, il est entre-temps pourvu à la présente réglementation » (*Parl. Dok.*, Kammer, 2020-2021, DOC 55-1677/001, SS. 10-11).

B.4.2.3. Artikel 11 des Gesetzes vom 22. Dezember 2020 wurde durch Artikel 11 des Zusammenarbeitsabkommens vom 12. März 2021 aufgehoben.

B.4.3. In der Präambel des königlichen Erlasses vom 24. Dezember 2020 ist angegeben, dass die Impfdatenbank von der Interministeriellen Konferenz Volksgesundheit am 3. Dezember 2020 bestimmt wurde (*Belgisches Staatsblatt* vom 24. Dezember 2020, S. 94404). Artikel 1 Nr. 2 des königlichen Erlasses vom 24. Dezember 2020 definiert die « Impfdatenbank » als « die Datenbank, die von der Interministeriellen Konferenz Volksgesundheit aufgrund von Artikel 11 des Gesetzes vom 22. Dezember 2020 über verschiedene Maßnahmen in Bezug auf Antigen-Schnelltests und über die Registrierung und Verarbeitung von Daten in Bezug auf Impfungen im Rahmen der Bekämpfung der COVID-19 Pandemie bestimmt wurde ».

Zu dieser Datenbank heißt es in den Vorarbeiten zum Gesetz vom 22. Dezember 2020:

« La proposition de loi à l'examen confère d'urgence un fondement légal à l'obligation d'enregistrer et de collecter les données relatives à la vaccination. Cet enregistrement est nécessaire pour pouvoir contrôler tous les aspects de la gestion de la crise. Il a été décidé d'inclure tous les enregistrements des différentes vaccinations dans la banque de données de vaccination flamande VaccinNet » (*Parl. Dok.*, Kammer, 2020-2021, DOC 55-1677/002, S. 4).

B.4.4.1. In einem Vereinbarungsprotokoll vom 27. Januar 2021 zwischen dem Föderalstaat, der Flämischen Gemeinschaft, der Französischen Gemeinschaft, der Deutschsprachigen Gemeinschaft, der Gemeinsamen Gemeinschaftskommission, der Wallonischen Region und der Französischen Gemeinschaftskommission « über die Verarbeitung von Daten im Zusammenhang mit Impfungen gegen COVID-19 » (nachstehend: Vereinbarungsprotokoll vom 27. Januar 2021) wurde der Inhalt der Bestimmungen des königlichen Erlasses vom 24. Dezember 2020 größtenteils übernommen. In der Präambel zu diesem Vereinbarungsprotokoll heißt es, dass dieses Protokoll « unter Beachtung der Verteilung der Zuständigkeiten, die den verschiedenen Befugnisebenen nach dem Sondergesetz zur Reform der Institutionen zugewiesen wurden, dank einer intensiven Zusammenarbeit innerhalb der Interministeriellen Konferenz, die einer langen Tradition der Zusammenarbeit innerhalb der Interministeriellen Konferenz Gesundheit zwischen den verschiedenen Befugnisebenen unseres Landes folgt, erreicht werden konnte » und dass « im Rahmen der Impfung gegen COVID-19 eine Registrierung der Impfdaten in einer gemeinsamen Datenbank durch die flämischen, Brüsseler, wallonischen und deutschsprachigen Impfberechtigten für verschiedene Zwecke absolut notwendig ist » (*Belgisches Staatsblatt* vom 11. Februar 2021, S. 13033).

In Artikel 1 Nr. 3 des Vereinbarungsprotokolls vom 27. Januar 2021 ist « Vaccinnet » definiert als « das Registrierungssystem, das in Artikel 9 des Erlasses der Flämischen Regierung vom 16. Mai 2014 zur Festlegung verschiedener Bestimmungen zur Ausführung des [flämischen] Dekrets vom 21. November 2003 über präventive Gesundheitspolitik und zur Abänderung der Ausführungserlasse zu diesem Dekret erwähnt ist ». Gemäß Artikel 43 des vorerwähnten Dekrets vom 21. November 2003 müssen die Impfberechtigten an dem Registrierungssystem « Vaccinnet » mitwirken, wenn die Flämische Regierung auf der Grundlage ihrer Zuständigkeit im Bereich Gesundheitspolitik ein Impfschema erstellt, das die für die Bevölkerung empfohlenen Impfungen wiedergibt.

Die in dem Vereinbarungsprotokoll vom 27. Januar 2021 erwähnte Datenbank « Vaccinnet » stellt daher eine Erweiterung der bestehenden Datenbank « Vaccinnet », die auf der Ebene der Flämischen Gemeinschaft eingerichtet wurde, bezüglich der Impfungen gegen COVID-19 dar. Die Aufteilung der Entwicklungskosten von « Vaccinnet » wurde in Artikel 6 des zwischen der Föderalregierung und den in den Artikeln 128, 130 und 135 der Verfassung erwähnten Behörden abgeschlossenen Vereinbarungsprotokolls vom 9. Februar 2022 « bezüglich der Kofinanzierung des Impfprogramms gegen COVID-19 » festgelegt.

B.4.4.2. Artikel 11 des Vereinbarungsprotokolls vom 27. Januar 2021 bestimmt:

« Le présent protocole d'accord n'est pas un accord de coopération au sens de l'article 92bis de la loi spéciale de réformes institutionnelles du 8 août 1980. Les parties se proposent, sur la base des dispositions du présent protocole d'accord, de parvenir à un accord de coopération pour le 21 avril 2021 ».

Artikel 12 des Vereinbarungsprotokolls vom 27. Januar 2021 bestimmt:

« Le présent protocole d'accord produit ses effets à dater du 24 décembre 2020 et cesse ses effets le jour où entre en vigueur un accord de coopération entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre la COVID-19 ».

B.5. Nach seinem Artikel 12 Absatz 1 ist das Zusammenarbeitsabkommen vom 12. März 2021 wirksam ab dem 24. Dezember 2020, was die Bestimmungen betrifft, deren Inhalt dem des königlichen Erlasses vom 24. Dezember 2020 über die Registrierung und Verarbeitung von

Daten über Impfungen gegen COVID-19 entspricht, und ab dem 11. Februar 2021, was die anderen Bestimmungen betrifft.

Nach Artikel 9 des königlichen Erlasses vom 24. Dezember 2020 und Artikel 12 des Vereinbarungsprotokolls vom 27. Januar 2021 sind der königliche Erlass vom 24. Dezember 2020 und das Vereinbarungsprotokoll vom 27. Januar 2021 am Tag des Inkrafttretens des Zusammenarbeitsabkommens vom 12. März 2021, das heißt am 22. April 2021, unwirksam geworden.

B.6. Die sieben angefochtenen Rechtsvorschriften (nachstehend: angefochtene Akte) beschränkten sich auf die Billigung des Zusammenarbeitsabkommens vom 12. März 2021.

In Bezug auf die Zulässigkeit ratione temporis der Klage

B.7. Die Wallonische Regierung, die Flämische Regierung, die Regierung der Französischen Gemeinschaft, die Regierung der Deutschsprachigen Gemeinschaft, das Kollegium der Französischen Gemeinschaftskommission und das Vereinigte Kollegium der Gemeinsamen Gemeinschaftskommission sind der Auffassung, dass die am 7. Oktober 2021 eingereichte Klage auf Nichtigkeitserklärung offensichtlich *ratione temporis* unzulässig ist, insofern sie gegen das Zustimmungsdekret Französischen Gemeinschaft vom 25. März 2021, veröffentlicht im *Belgischen Staatsblatt* vom 6. April 2021, gerichtet ist.

B.8.1. Damit die Voraussetzungen des Artikels 3 § 1 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof erfüllt sind, muss eine Nichtigkeitsklage binnen einer Frist von sechs Monaten nach der Veröffentlichung der angefochtenen Norm im *Belgischen Staatsblatt* eingereicht werden.

B.8.2. In der vorerwähnten Bestimmung wird keine Unterscheidung nach dem Einsetzen der Frist für die Klage auf Nichtigkeitserklärung der angefochtenen Norm, je nachdem, ob sie ein Zusammenarbeitsabkommen billigt oder nicht, vorgenommen.

Im Gegensatz zu dem, was die klagende Partei anführt, setzt die Frist, um eine Klage auf Nichtigkeitserklärung gegen Zustimmungsakte zu einem Zusammenarbeitsabkommen

einzureichen, nicht ab dem Inkrafttreten des besagten Zusammenarbeitsabkommens ein, sondern beginnt ab dem Tag der Veröffentlichung der angefochtenen Akte zu laufen.

B.8.3. Der Gerichtshof hat bereits in mehreren vorherigen Entscheiden darauf hingewiesen, dass - in Ermangelung einer näheren Präzisierung im Sondergesetz vom 6. Januar 1989 und in Analogie zu der Regelung von Artikel 54 des Gerichtsgesetzbuches - zur Bestimmung der für die Einreichung einer Klage auf Nichtigklärung oder einstweilige Aufhebung geltenden Frist ab dem Soundsovielten bis zum Tag vor dem Soundsovielten zu rechnen ist (siehe Entscheid Nr. 125/2012 vom 18. Oktober 2012, ECLI:BE:GHCC:2012:ARR.125, B.2; Entscheid Nr. 169/2016 vom 22. Dezember 2016, ECLI:BE:GHCC:2016:ARR.169, B.2).

Das Zustimmungsdekret der Französischen Gemeinschaft vom 25. März 2021 wurde im *Belgischen Staatsblatt* vom 6. April 2021 veröffentlicht. Die Frist, um eine Klage gegen diesen Akt einzureichen, hat somit am 7. April 2021 begonnen und ist am 6. Oktober 2021 abgelaufen. Daraus folgt, dass die mit einer am 7. Oktober 2021 bei der Post aufgegebenen Klageschrift eingereichte Klage auf Nichtigklärung offensichtlich unzulässig ist.

B.8.4. Die Klage auf Nichtigklärung, insofern sie gegen das Zustimmungsdekret Französischen Gemeinschaft vom 25. März 2021 gerichtet ist, ist *ratione temporis* unzulässig.

In Bezug auf den Umfang der Nichtigkeitsklage

B.9.1. Um den Erfordernissen nach Artikel 6 des Sondergesetzes vom 6. Januar 1989 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 die fraglichen Bestimmungen verletzt würden.

B.9.2. Der Gerichtshof bestimmt den Umfang der Nichtigkeitsklage anhand des Inhalts der Klageschrift, insbesondere auf Grundlage der Darlegung der Klagegründe. Der Gerichtshof beschränkt seine Prüfung auf jene Bestimmungen, gegen die tatsächlich auch Einwände erhoben wurden.

B.10.1. Aus der Begründung des einzigen Klagegrunds geht hervor, dass die Beschwerdegründe der klagenden Partei nur gegen die angefochtenen Akte gerichtet sind, insofern sie bestimmte Bestimmungen des Zusammenarbeitsabkommens vom 12 März 2021 billigen, die die Registrierung und die Verarbeitung personenbezogener Daten in der Datenbank « Vaccinnet » regeln und die von der klagenden Partei in ihrem Klagegrund ausdrücklich angegeben werden:

- Artikel 2 § 2, der sich auf die Registrierung der Impfdaten bezieht;
- Artikel 3 § 2, der die in « Vaccinnet » erfassten Impfdaten bestimmt;
- Artikel 4 § 2, der die Zwecke für die Verarbeitung der in Artikel 3 § 2 erwähnten Daten festlegt;
- Artikel 5, der die Übermittlung von in « Vaccinnet » erfassten Daten an Dritte erlaubt;
- Artikel 6 § 2, der die Dauer der Aufbewahrung der in Artikel 3 § 2 erwähnten Daten festlegt;
- Artikel 12, der den Tag des Inkrafttretens der Bestimmungen des Zusammenarbeitsabkommens vom 12. März 2021 festlegt.

B.10.2. Bei ihrer Kritik an diesen Bestimmungen in ihrem einzigen Klagegrund formuliert die klagende Partei jedoch keinen Beschwerdegrund weder gegen die grundsätzliche Registrierung der Impfdaten noch gegen die in « Vaccinnet » erfassten Impfdaten. Abgesehen von einer allgemeinen Kritik legt sie nicht dar, inwiefern die angefochtenen Akte, indem sie die Artikel 2 § 2 und 3 § 2 des Zusammenarbeitsabkommens vom 12. März 2021 billigen, gegen die im Klagegrund erwähnten Bestimmungen verstoßen würden.

Insofern er sich auf diese Bestimmungen bezieht, entspricht der einzige Klagegrund deshalb nicht den Erfordernissen von Artikel 6 des Sondergesetzes vom 6. Januar 1989.

B.10.3. Folglich beschränkt der Gerichtshof seine Prüfung der gegen die angefochtenen Akte gerichteten Nichtigkeitsklage, insofern damit die Artikel 4 § 2, 5 und 6 § 2 des Zusammenarbeitsabkommens vom 12. März 2021 und Artikel 12 des vorerwähnten Zusammenarbeitsabkommens, insoweit dieser den Tag des Inkrafttretens der vorerwähnten Artikel 4 § 2, 5 und 6 § 2 festlegt, gebilligt werden.

Die Nichtigkeitsklage ist dementsprechend unzulässig, insofern sie gegen die angefochtenen Akte gerichtet ist, insoweit damit die anderen Bestimmungen des vorerwähnten Zusammenarbeitsabkommens gebilligt werden.

B.10.4. Der Gerichtshof erinnert daran, dass er die angefochtenen Akte nicht sachdienlich prüfen kann, ohne in seine Prüfung den Inhalt der relevanten Bestimmungen des vorerwähnten Zusammenarbeitsabkommens einzubeziehen.

In Bezug auf das Interesse der klagenden Partei

B.11. Die klagende Partei führt zur Begründung ihres Interesses an der Klageerhebung an, dass sie eine natürliche Person ist, die in Belgien wohnt, und dass sie sich gegen COVID-19 impfen lassen könnte, sodass die angefochtenen Akte sie unmittelbar und ungünstig beeinflussen können. Wenn sie sich entscheide, sich impfen zu lassen, würden nämlich ihr Name und ihre verschiedenen personenbezogenen Daten in « Vaccinnet » aufgenommen und damit ihr Recht auf Achtung des Privatlebens in Verbindung mit dem Grundsatz der Nichtrückwirkung der Gesetze missachtet. Wenn sie sich hingegen entscheide, sich nicht impfen zu lassen, bestehe eine ernsthafte Gefahr, dass mit ihrer fehlenden Impfung Einschränkungen verbunden seien.

B.12. Der Ministerrat, die Wallonische Regierung, die Flämische Regierung, die Regierung der Französischen Gemeinschaft, die Regierung der Deutschsprachigen Gemeinschaft, das Kollegium der Französischen Gemeinschaftskommission und das Vereinigte Kollegium der Gemeinsamen Gemeinschaftskommission bestreiten das Interesse der klagenden Partei an der Klageerhebung, da sie der Auffassung sind, dass ihre Klage einer Popularklage gleichkomme.

B.13. Die Verfassung und das Sondergesetz vom 6. Januar 1989 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 angefochtene Rechtsnorm unmittelbar und ungünstig beeinflusst werden könnte.

B.14.1. Nach dem nicht angefochtenen Artikel 2 § 1 des Zusammenarbeitsabkommens vom 12. März 2021 soll jede natürliche Person, die sich auf belgischem Staatsgebiet aufhält, über einen Impfcodes eine Einladung zur Impfung gegen COVID-19 gemäß der von den zuständigen Behörden festgelegten Impfstrategie erhalten. Dieser Impfcodes ohne besondere Bedeutung wird von der gemäß dem nicht angefochtenen Artikel 3 § 1 des Zusammenarbeitsabkommens vom 12. März 2021 geregelten Datenbank generiert.

Nach Artikel 2 § 2 des Zusammenarbeitsabkommens vom 12. März 2021 führt jede Impfung zur Registrierung der in Artikel 3 § 2 des Zusammenarbeitsabkommens vom 12. März 2021 erwähnten Impfdaten in « Vaccinnet ». Alle Personen, die sich gegen COVID-19 impfen lassen, unterliegen folglich der automatischen Registrierung ihrer Impfdaten in der Datenbank « Vaccinnet » und der Verarbeitung dieser Daten gemäß den Regelungen, die in diesem Zusammenarbeitsabkommen vorgesehen sind.

In ihrer Eigenschaft als natürliche Person, die sich auf belgischem Staatsgebiet aufhält, ist die klagende Partei gemäß den angefochtenen Akten zur Billigung des Zusammenarbeitsabkommens vom 12. März 2021 zwangsläufig dazu eingeladen worden, sich impfen zu lassen, und sie konnte die Einladung zur Impfung nur dadurch annehmen, dass sie es akzeptiert, dass ihre Impfdaten in « Vaccinnet » registriert und verarbeitet werden. Die Auswirkungen der angefochtenen Akte im Bereich der Verarbeitung der Impfdaten können daher die Entscheidung der klagenden Partei in Bezug auf ihre Impfung gegen COVID-19 unmittelbar beeinflussen.

B.14.2. Aus dem Vorstehenden ergibt sich, dass die angefochtenen Akte die klagende Partei bei ihrer Entscheidung, sich impfen zu lassen, unmittelbar und ungünstig beeinflussen können.

B.14.3. Im Übrigen beschränkt sich das Zusammenarbeitsabkommen vom 12. März 2021 darauf, das gemeinsame System zur Registrierung der Daten der Impfung gegen COVID-19 im

Staatsgebiet Belgiens zu regeln. Dieses Zusammenarbeitsabkommen führt keine Impflpflicht ein, da die in B.2.2 dargelegte Impfstrategie auf einer freiwilligen und kostenlosen Impfung beruht.

Im Gegensatz zu den Ausführungen der klagenden Partei sehen die angefochtenen Akte keine Folge vor, die mit dem Fehlen einer Impfung verbunden wäre. Die Auswirkungen eines Impfbzertifikats aber auch eines Test- und Genesungszertifikats, um ein CST zu erhalten, sind in den in B.2.3.4 zitierten Zusammenarbeitsabkommen vom 14. Juli 2021, 27. September 2021 und 28. Oktober 2021 bestimmt. Die klagende Partei weist nicht nur nicht nach, dass die Einschränkungen, die sie geltend macht und die sich aus dem Fehlen der Impfung ergäben, wirklich bestehen - was genügen würde, um festzustellen, dass der geltend gemachte Nachteil rein hypothetisch ist -, sondern diese eventuellen Einschränkungen stellen auch keinen Nachteil dar, der sich unmittelbar aus den durch die vorliegende Klage angefochtenen Akten ergeben würde.

Insofern sie die mit der Nichtimpfung gegen COVID-19 verbundenen Folgen geltend macht, weist die klagende Partei nicht das erforderliche Interesse nach.

Zur Hauptsache

B.15. Der einzige Klagegrund ist abgeleitet aus einem Verstoß gegen Artikel 22 der Verfassung in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union, mit den Artikeln 5, 6, 9 und 35 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), sowie in Verbindung mit dem Grundsatz der Nichtrückwirkung der Gesetze.

B.16.1. 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.16.2. 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.16.3. 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.16.4. 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.

Dieses Recht hat eine weitreichende Tragweite und umfasst unter anderem das Recht auf körperliche Unversehrtheit der Person (EuGHMR, Große Kammer, 8. April 2021, *Vavříčka u.a. gegen Tschechische Republik*, ECLI:CE:ECHR:2021:0408JUD004762113, § 261) und den Schutz personenbezogener Daten und persönlicher Informationen in Bezug auf die Gesundheit (EuGHMR, 25. Februar 1997, *Z. gegen Finnland*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; 10. Oktober 2006, *L.L. gegen Frankreich*, ECLI:CE:ECHR:2006:1010JUD000750802, § 32; 27. Februar 2018, *Mockuté gegen Litauen*, ECLI:CE:ECHR:2018:0227JUD006649009, § 93). Aus der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte ergibt sich, dass unter anderem die folgenden Daten und Informationen über die Person von diesem Recht geschützt sind: Name, Adresse, berufliche Aktivitäten, persönliche Beziehungen, digitale Fingerabdrücke, Kamerabilder, Fotos, Kommunikationsdaten, DNA-Daten, gerichtliche Daten

(Verurteilung oder Verdacht), Finanzdaten, Informationen über Vermögenswerte und medizinische Daten (siehe u.a. EuGHMR, 26. März 1987, *Leander gegen Schweden*, ECLI:CE:ECHR:1987:0326JUD000924881, §§ 47-48; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, ECLI:CE:ECHR:2008:1204JUD003056204, §§ 66-68; 17. Dezember 2009, *B.B. gegen Frankreich*, ECLI:CE:ECHR:2009:1217JUD000533506, § 57; 10. Februar 2011, *Dimitrov-Kazakov gegen Bulgarien*, ECLI:CE:ECHR:2011:0210JUD001137903, §§ 29-31; 18. Oktober 2011, *Khelili gegen Schweiz*, ECLI:CE:ECHR:2011:1018JUD001618807, §§ 55-57; 9. Oktober 2012, *Alkaya gegen Türkei*, ECLI:CE:ECHR:2012:1009JUD004281106, § 29; 18. April 2013, *M.K. gegen Frankreich*, ECLI:CE:ECHR:2013:0418JUD001952209, § 26; 18. September 2014, *Brunet gegen Frankreich*, ECLI:CE:ECHR:2014:0918JUD002101010, § 31; 13. Oktober 2020, *Frâncu gegen Rumänien*, ECLI:CE:ECHR:2020:1013JUD006935613, § 51).

Der Schutz personenbezogener Daten bezüglich der Gesundheit ist nicht nur von grundlegender Bedeutung für das Recht auf Achtung des Privatlebens der Person, sondern auch für ihr Vertrauen in den Gesundheitsdienst (EuGHMR, 25. Februar 1997, *Z. gegen Finnland*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95). Ohne diesen Schutz könnten Personen darauf verzichten, sensible und persönliche Informationen mit Pflegebringern oder mit Gesundheitsdiensten zu teilen, womit sie nicht nur ihre eigene Gesundheit, sondern im Falle von Infektionskrankheiten auch die Gesellschaft gefährden können (ebenda, § 95).

B.16.5. 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*, ECLI:CE:ECHR:1994:1027JUD001853591, § 31; Große Kammer, 12. November 2013, *Söderman gegen Schweden*, ECLI:CE:ECHR:2013:1112JUD000578608, § 78).

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*, ECLI:CE:ECHR:2017:0126JUD004278806, § 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*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, ECLI:CE:ECHR:2008:1204JUD003056204, § 103; 26. Januar 2017, *Surikov gegen Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 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 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*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

B.16.6. 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 (EuGH, Große Kammer, 9. November 2010, C-92/09 und C-93/09, *Volker und Markus Schecke GbR u.a.*, ECLI:EU:C:2010:662), während Artikel 8 der Charta einen spezifischen Rechtsschutz für personenbezogene Daten bietet.

B.16.7. 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 bestimmbar natürliche Person betrifft (EuGH, Große Kammer, 9. November 2010, C-92/09 und C-93/09, *Volker und Markus Schecke GbR u.a.*, ECLI:EU:C:2010:662, Randnr. 52; 16. Januar 2019, C-496/17, *Deutsche Post AG*, ECLI:EU:C:2019:26, Randnr. 54).

B.16.8. Auch die in den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union verankerten Grundrechte können keine uneingeschränkte Geltung beanspruchen (EuGH, Große Kammer, 16. Juli 2020, C-311/18, *Data Protection Commissioner*, ECLI:EU:C:2020:559, Randnr. 172).

Nach Artikel 52 Absatz 1 Satz 1 der Charta der Grundrechte der Europäischen Union müssen Einschränkungen der Ausübung der darin garantierten Rechte und Freiheiten, einschließlich insbesondere des durch deren Artikel 7 gewährleisteten Rechts auf Achtung des Privatlebens und des in Artikel 8 verankerten Rechts auf Schutz personenbezogener Daten, gesetzlich vorgesehen sein, den Wesensgehalt dieser Rechte achten und unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sein sowie einer dem Gemeinwohl dienenden Zielsetzung oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen (EuGH, Große Kammer, 6. Oktober 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, Randnr. 64). Im selben Sinne müssen nach Artikel 23 der DSGVO Beschränkungen der darin genannten Verpflichtungen der für die Verarbeitung Verantwortlichen und der Rechte der betroffenen Personen gesetzlich vorgesehen sein, den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen

Gesellschaft eine notwendige und verhältnismäßige Maßnahme zur Verwirklichung des verfolgten Ziels darstellen, sowie die in Absatz 2 formulierten spezifischen Anforderungen erfüllen (EuGH, Große Kammer, 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u.a.*, ECLI:EU:C:2020:791, Randnrn. 209-210; 10. Dezember 2020, C-620/19, *Land Nordrhein-Westfalen*, ECLI:EU:C:2020:1011, Randnr. 46).

B.16.9. 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 Verarbeitung personenbezogener Daten im Gesetz, im Dekret oder in der Ordonnanz selbst festgelegt sein. Diesbezüglich sind die wesentlichen Elemente unabhängig von dem betroffenen Bereich grundsätzlich die folgenden Elemente: (1) die Kategorie der verarbeiteten Daten, (2) die betroffene Personenkategorie, (3) der mit der Verarbeitung verfolgte Zweck, (4) die Kategorie der Personen, die Zugriff auf die verarbeiteten Daten haben, und (5) die maximale Dauer der Aufbewahrung der Daten (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.16.10. 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 der Grundrechte der Europäischen Union ebenfalls die Verpflichtung auferlegt, dass die Einmischung in das Recht auf Achtung des Privatlebens und das Recht 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 in das Recht auf Achtung des Privatlebens erlaubt.

Auf dem Gebiet des Schutzes personenbezogener Daten 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*, ECLI:CE:ECHR:2000:0504JUD002834195, § 57; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, ECLI:CE:ECHR:2008:1204JUD003056204, § 99). Das Erfordernis, dass die Einschränkung gesetzlich vorgesehen sein muss, bedeutet insbesondere, dass die gesetzliche Grundlage für den Eingriff in diese Rechte den Umfang, in dem die Ausübung des betreffenden Rechts eingeschränkt wird, selbst festlegen muss (EuGH, 6. Oktober 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, Randnr. 65).

Deshalb muss es jeder Person möglich sein, sich ein ausreichend klares Bild von den verarbeiteten Daten, den an einer bestimmten Datenverarbeitung beteiligten Personen sowie den Bedingungen und den Zwecken der Verarbeitung zu machen.

B.16.11. 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 35 der DSGVO mit der Überschrift « Datenschutz-Folgenabschätzung » bestimmt:

« (1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind ».

B.16.12. Die Nichtrückwirkung von Gesetzen ist eine Garantie zur Vermeidung von Rechtsunsicherheit. Diese Garantie erfordert es, dass der Inhalt des Rechtes vorhersehbar und zugänglich ist, so dass der Rechtsuchende in vernünftigem Maße die Folgen einer bestimmten Handlung zu dem Zeitpunkt vorhersehen kann, an dem die Handlung ausgeführt wird. Die

Rückwirkung ist nur dann gerechtfertigt, wenn sie unerlässlich ist zur Verwirklichung einer Zielsetzung allgemeinen Interesses.

Wenn sich herausstellt, dass die Rückwirkung außerdem zum Ziel oder zur Folge hat, dass der Ausgang von Gerichtsverfahren in einem bestimmten Sinne beeinflusst wird oder dass die Gerichte daran gehindert werden, über eine bestimmte Rechtsfrage zu befinden, verlangt es die Beschaffenheit des betreffenden Grundsatzes, dass außergewöhnliche Umstände oder zwingende Gründe allgemeinen Interesses dieses Eingreifen des Gesetzgebers rechtfertigen, das zum Nachteil einer Kategorie von Bürgern die allen gebotenen Rechtsprechungsgarantien beeinträchtigt.

B.17. Die Beschwerdegründe der klagenden Partei beziehen sich auf folgende Aspekte:

I. Die Verarbeitungszwecke der Impfdaten, die in Artikel 4 § 2 erwähnt sind (erster Teil) (B.18 bis B.24);

II. die dem Informationssicherheitsausschuss erteilte Ermächtigung, die Übermittlung von personenbezogenen Daten an Dritte zu genehmigen, die in Artikel 5 erwähnt ist (erster Teil) (B.25 bis B.32);

III. die Dauer der Aufbewahrung der in « Vaccinnet » gespeicherten Daten, die in Artikel 6 erwähnt ist (zweiter Teil) (B.33 bis B.38);

IV. das Fehlen einer nach Artikel 35 der DSGVO erforderlichen vorherigen Folgenabschätzung (zweiter Teil) (B.39 bis B.45);

V. die Rückwirkung des Zusammenarbeitsabkommens zum 24. Dezember 2020, die in Artikel 12 vorgesehen ist (dritter Teil) (B.46 bis B.50).

I. In Bezug auf die Verarbeitungszwecke der Impfdaten, die in Artikel 4 § 2 erwähnt sind (erster Teil)

B.18. Im ersten Teil des Klagegrunds vertritt die klagende Partei die Auffassung, dass die elf in Artikel 4 § 2 des Zusammenarbeitsabkommens vom 12. März 2021 festgelegten Zwecke nicht ausreichend « festgelegt und eindeutig » sind, sodass das Legalitätsprinzip und der Grundsatz der Vorhersehbarkeit der wesentlichen Elemente der Verarbeitung von sensiblen personenbezogenen Daten nicht beachtet werden. Sie beanstandet insbesondere die weit gefasste Beschaffenheit des unter Nr. 1 erwähnten Zwecks sowie die Erforderlichkeit des unter Nr. 11 erwähnten Zwecks.

B.19. Artikel 4 § 2 des Zusammenarbeitsabkommens vom 12. März 2021 bestimmt:

«Die Verarbeitung der in Artikel 3 § 2 erwähnten personenbezogenen Daten dient folgenden Verarbeitungszwecken:

1° Gesundheitspflege- und Behandlungsleistungen im Sinne von Artikel 9 Nr. 2 Buchstabe *h*) der Datenschutz-Grundverordnung, was ausschließlich durch die Impfung und die Maßnahmen zur Unterstützung, Information und Sensibilisierung der Bürger im Zusammenhang mit der Impfung bezweckt wird;

2° Pharmakovigilanz von Impfstoffen gegen COVID-19 gemäß Artikel 12^{sexies} des Gesetzes vom 25. März 1964 über Arzneimittel und den ausführlichen Leitlinien, die von der Europäischen Kommission in ‘Modul VI - Sammlung, Verwaltung und Weitergabe von Berichten über vermutete Nebenwirkungen von Arzneimitteln (GVP)’ in der neuesten verfügbaren Fassung veröffentlicht wurden und auf die in Artikel 4 § 1 Absatz 3 Nr. 3 des Gesetzes vom 20. Juli 2006 über die Schaffung und die Arbeitsweise der Föderalagentur für Arzneimittel und Gesundheitsprodukte Bezug genommen wird;

3° Rückverfolgbarkeit von Impfstoffen gegen COVID-19, um die Weiterverfolgung des ‘Rapid Alert Systems für Vigilanzfragen’ und des ‘Rapid Alert Systems für Qualitätsfragen’, wie in Artikel 4 § 1 Absatz 3 Nr. 3 Buchstabe *e*) und Nr. 4 Buchstabe *j*) des Gesetzes vom 20. Juli 2006 über die Schaffung und die Arbeitsweise der Föderalagentur für Arzneimittel und Gesundheitsprodukte erwähnt, zu gewährleisten;

4° Verwaltung der COVID-19-Impfschemas pro zu impfende beziehungsweise geimpfte Person und Planung der Impftermine, unter anderem durch die Impfzentren;

5° logistische Organisation der Impfung gegen COVID-19, nach Anonymisierung der Daten oder zumindest Pseudonymisierung der Daten, falls eine Anonymisierung die logistische Organisation nicht ermöglichen würde;

6° Ermittlung der anonymen Durchimpfungsrate der Bevölkerung gegen COVID-19;

7° Organisation der Kontaktermittlung in Ausführung 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;

8° Durchführung der Überwachung und Kontrolle der Impfstoffe nach der Zulassung in Übereinstimmung mit den von der Weltgesundheitsorganisation empfohlenen guten Praktiken nach Anonymisierung der Daten oder zumindest Pseudonymisierung der Daten, falls eine Anonymisierung die Überwachung und Kontrolle nach der Zulassung nicht ermöglichen würde;

9° unbeschadet der Vorschriften über die Krankenversicherung, Berechnung der Aufteilung der Impfkosten zwischen dem Föderalstaat und den föderierten Teilgebieten nach Anonymisierung der Daten oder zumindest Pseudonymisierung der Daten, falls eine Anonymisierung die Berechnung der Aufteilung nicht ermöglichen würde;

10° Durchführung wissenschaftlicher oder statistischer Studien gemäß Artikel 89 § 1 der Datenschutz-Grundverordnung und gegebenenfalls Artikel 89 §§ 2 und 3 der Datenschutz-Grundverordnung und Titel 4 des Gesetzes vom 30. Juli 2018 über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten nach Anonymisierung oder zumindest Pseudonymisierung, falls eine Anonymisierung die Durchführung der wissenschaftlichen oder statistischen Studie nicht ermöglichen würde;

11° Information und Sensibilisierung von Personen bezüglich der Impfung gegen COVID-19 durch Pflegeanbieter und Versicherungsträger ».

B.20.1. Bezüglich der in Artikel 4 erwähnten Zwecke heißt es in den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 12. März 2021:

« In Artikel 4 werden die Verarbeitungszwecke für die Datenbanken beschrieben, die im Allgemeinen wie folgt lauten:

- Bereitstellung einer qualitativ hochwertigen Pflege für die betreffende Person, was das ausschließliche Ziel der Impfung und der Maßnahmen zur Unterstützung, Information und Sensibilisierung der Bürger im Zusammenhang mit der Impfung ist,

- Pharmakovigilanz,

- Rückverfolgbarkeit von Impfstoffen,

- Verwaltung der COVID-19-Impfschemas und Planung der Impftermine, unter anderem durch die Impfzentren und die Pflegeanbieter,

- logistische Organisation der Impfung gegen COVID-19; in diesem Zusammenhang ist es sinnvoll, darauf hinzuweisen, dass zur Erreichung dieses Zwecks sowohl die Impfcode-Datenbank als auch die Datenbank für die Registrierung von Impfungen erforderlich sind, wobei letztere es insbesondere ermöglicht, erstere zu speisen, zum Beispiel um zu vermeiden, dass bereits geimpfte Personen erneut eingeladen werden, oder um den Bedarf an

Impfstoffen oder medizinischem Personal hinsichtlich noch zu verabreichender Impfungen zu ermitteln,

- Ermittlung der anonymen Durchimpfungsrate der Bevölkerung gegen COVID-19,
- Organisation der Kontaktrückverfolgung,
- Durchführung der Überwachung und Kontrolle der Impfstoffe nach der Zulassung,
- Berechnung der Aufteilung der Impfkosten zwischen dem Föderalstaat und den föderierten Teilgebieten,
- Unterstützung der wissenschaftlichen Forschung, insbesondere zur Wirksamkeit und Sicherheit von Impfstoffen,
- Information und Sensibilisierung von Personen bezüglich der Impfung gegen COVID-19 durch Gesundheitsinspektionsdienste der föderierten Teilgebiete, Pflegeanbieter und Versicherungsträger, um einen höchstmöglichen Impfgrad zu erreichen,
- Einladung und Unterstützung beim Einladungsprozess zur Impfung gegen COVID-19 durch Pflegeanbieter, Versicherungsträger, Impfzentren, die Föderalbehörde, die zuständigen föderierten Teilgebiete und lokale Behörden.

In Bezug auf den Zweck der Überwachung und Kontrolle der Impfstoffe nach der Zulassung können folgende nähere Angaben gemacht werden.

Studien zur Akzeptanz und Verwendung der Impfstoffe und zur Impfabdeckung geben Auskunft darüber, wie viele Menschen bereit sind, sich impfen zu lassen, und wie viele tatsächlich geimpft werden. Insbesondere ermöglichen die Studien zur Impfabdeckung, den Anteil der Geimpften in bestimmten Risikogruppen, zum Beispiel ältere Menschen oder Menschen mit spezifischen Grunderkrankungen, abzuschätzen. Diese Studien geben Aufschluss über die Einstellung der Bevölkerung zu den Impfstoffen und helfen, die zu behebenden Mängel des Impfprogramms zu identifizieren.

Die Überwachung der Wirksamkeit, Seroprävalenz und Immunogenität der Impfstoffe ermöglicht eine Bewertung der Fähigkeit des Impfstoffs, eine Immunreaktion auszulösen und einer Infektion langfristig und im Fall neuer zirkulierender Virenstämme vorzubeugen.

Schließlich ist es entscheidend, die Qualität der Impfstoffe zu kontrollieren und ein System einzurichten, das in der Lage ist, späte oder seltene Nebenwirkungen zu erkennen, um die Sicherheit der Impfstoffe weiterhin zu gewährleisten.

Insgesamt werden die Ergebnisse der nach der Zulassung durchgeführten Kontrolle verwendet, um die Impfpolitik zu orientieren und die Gesundheitsfachkräfte und die allgemeine Bevölkerung über die Ergebnisse des belgischen COVID-19-Impfprogramms zu informieren.

Diese Überwachung und Kontrolle der Impfstoffe nach der Zulassung erfolgt in jedem Fall in Übereinstimmung mit den diesbezüglich von der Weltgesundheitsorganisation empfohlenen guten Praktiken.

Hervorzuheben ist die Bedeutung des Zusammenhangs mit der Kontaktrückverfolgung, da die Organisation der Rückverfolgung eines der Ziele ist. Die anvisierten Szenarien, die eine Verknüpfung von Impfung und Kontaktermittlung ermöglichen, müssen dem ausschließlichen Zweck der Ermittlung infektiöser Kontakte und der Nachverfolgung der Impfung dienen. Insbesondere folgende Szenarien sind denkbar:

- Die durch das Kontaktzentrum zu erteilenden Empfehlungen können sich unterscheiden, je nachdem, ob jemand geimpft wurde oder nicht.

- Die Quelle wurde geimpft, hat aber eine Reihe von Kontakten infiziert; dies ist ein Fall von Impfversagen oder ein Variantenstamm, gegen den der Impfstoff nicht schützt. Es handelt sich daher um eine sehr wichtige Information für die Volksgesundheit.

- Die Quelle wurde nicht geimpft, sodass sich andere Personen infiziert haben.

- Die Kontakte sind wahrscheinlich geimpft, wodurch die Epidemie abebben kann, da sich der Impfstoff als wirksame Vorbeugungsmaßnahme erweist.

- Die Kontakte sind nicht geimpft, sodass die Epidemie weiter aktiv kartiert werden muss.

Die Daten, die in diesem Rahmen von Vaccinnet an die Datenbank von Sciensano übermittelt werden, betreffen a priori die ENSS, den Impfstatus und die Art des Impfstoffs, wobei jedoch eine Flexibilität entsprechend den neuesten wissenschaftlichen Erkenntnissen über die Auswirkungen der Impfung auf das Infektionsrisiko erforderlich ist.

Darüber hinaus ist zu betonen, dass personenbezogene Daten notwendig sind, um die medizinische Nachsorge des Patienten in Bezug auf die Impfung gegen COVID-19 zu gewährleisten, da eine hohe Impfabdeckung in der Bevölkerung angesichts der beispiellosen Krise der COVID-19-Pandemie und auf Ebene des Einzelnen, der in der Lage sein muss, eine informierte Entscheidung für seine persönliche Gesundheit zu treffen, eine unabdingbare und grundlegende Voraussetzung für die öffentliche Gesundheit ist. Dies erfordert in der Tat eine Kombination aus allgemeinen und gezielten Informationen (auf Initiative des behandelnden Arztes oder des Versicherungsträgers für die eigenen Patienten beziehungsweise Mitglieder). Insbesondere ist es von größter Bedeutung, dass der Arzt (Hausarzt, Facharzt) auf der Grundlage seiner genauen Kenntnis der medizinischen Anamnese des ihm anvertrauten Patienten beurteilt, ob die Impfung des ordnungsgemäß aufgeklärten Patienten wichtig ist oder nicht. In diesem Zusammenhang ist zu betonen, dass ständig auf eine ausreichende Durchimpfungsrate (zum Beispiel 70 Prozent) zu achten ist und dass es wichtig ist, dies gezielt zu begleiten (über Kampagnen und auf individueller Ebene). Es versteht sich von selbst, dass es verboten ist, Personen zu kontaktieren, die ausdrücklich erklärt haben, den Impfstoff abzulehnen, wenn sie dies nicht wünschen.

Das Ziel, eine qualitativ hochwertige Pflege bereitzustellen, beinhaltet nicht, den Zugang zu einer qualitativ hochwertigen Versorgung in irgendeiner Weise aufgrund des Impfstatus einer Person zu beschränken oder mit Bedingungen zu verbinden.

Zu beachten ist auch, dass der Grad anonymer Impfungen gegen COVID-19 granular bestimmbar sein muss (zum Beispiel muss in Wohnpflegezentren zwischen dem Pflegepersonal und den Bewohnern unterschieden werden) und dass diese Bestimmung nicht immer mit

anonymisierten Daten oder zumindest, falls eine Anonymisierung nicht zielführend wäre, mit pseudonymisierten Daten erfolgen kann.

Darüber hinaus ist es sinnvoll, darauf hinzuweisen, dass alle Kategorien von Daten, die sowohl in der Impfcode-Datenbank als auch in der Datenbank für die Registrierung von Impfungen erfasst werden, prinzipiell für jeden der Zwecke verarbeitet und aufbewahrt werden können. Im Text des Zusammenarbeitsabkommens werden zudem die Fälle bestimmt, in denen nur anonymisierte oder zumindest, falls eine Anonymisierung nicht zielführend wäre, pseudonymisierte Daten betroffen sind.

Die im Rahmen des vorliegenden Zusammenarbeitsabkommens erhobenen Daten dürfen nicht für andere als die in diesem Abkommen vorgesehenen Zwecke verwendet werden.

Die im Rahmen des vorliegenden Zusammenarbeitsabkommens erhobenen Daten dürfen somit nicht zu anderen als den in diesem Artikel vorgesehenen Zwecken verwendet werden, und insbesondere nicht - aber nicht ausschließlich - zu polizeilichen, kommerziellen, steuerrechtlichen, strafrechtlichen oder staatssicherheitlichen Zwecken.

Schließlich muss die Verwendung der Daten aus den Datenbanken mit Artikel 14 der Europäischen Menschenrechtskonvention, Artikel 10 und 11 der Verfassung und dem Gesetz vom 10. Mai 2007 zur Bekämpfung bestimmter Formen der Diskriminierung übereinstimmen.

Jeder Nutzer des Gesundheitswesens hat immer das Recht, eine Impfbescheinigung zu erhalten. Diese Bescheinigung darf jedoch niemals zu einer Diskriminierung von Nutzern des Gesundheitswesens führen » (*Belgisches Staatsblatt* vom 12. April 2021, SS. 32404-32408; siehe auch *Parl. Dok.*, Kammer, 2020-2021, DOC 55-1853/001, SS. 9-13).

B.20.2. In ihrem Gutachten zum Vorentwurf des Gesetzes, das zum Gesetz vom 2. April 2021 zur Billigung des Zusammenarbeitsabkommens vom 12. März 2021 geworden ist, hat die Gesetzgebungsabteilung des Staatsrates bezüglich der Zwecke der Datenverarbeitung angemerkt:

« Le paragraphe 2, 9°, prévoit comme finalité de traitement

‘ la répartition des coûts de vaccination entre l’État fédéral et les entités fédérées, après anonymisation des données ou à tout le moins pseudonymisation des données dans l’hypothèse où l’anonymisation ne permettrait pas de réaliser le calcul de répartition ’.

Conformément au principe de minimisation des données, si l’enregistrement de données anonymisées suffit pour atteindre l’objectif poursuivi, il ne convient pas de prévoir la possibilité de pseudonymisation.

Interrogés quant aux hypothèses dans lesquelles l’anonymisation des données ne permettrait pas de réaliser le calcul de répartition des coûts de vaccination, les délégués ont précisé ce qui suit :

‘ In het kader van de regelgeving inzake de ziekteverzekering kan het nodig zijn over persoonsgegevens te beschikken ’.

Il n'est pas possible, à la lumière de cette réponse, de se prononcer quant à l'admissibilité du dispositif à l'examen. L'auteur de l'avant-projet est donc invité à préciser davantage, dans le commentaire de l'article, les situations dans lesquelles l'anonymisation des données ne permettrait pas de réaliser le calcul de répartition des coûts de vaccination » (ebenda, SS. 51-52; siehe auch *Parl. Dok.*, Flämisches Parlament, 2020-2021, Nr. 708/1, S. 88; *Parl. Dok.*, Wallonisches Parlament, 2020-2021, Nr. 509/1, S. 84; *Parl. Dok.*, Parlament der Deutschsprachigen Gemeinschaft, 2020-2021, Nr. 132/1, SS. 31-32; *Parl. Dok.*, Vereinigte Versammlung der Gemeinsamen Gemeinschaftskommission, 2020-2021, Nr. B-65/1, SS. 16-17; *Parl. Dok.*, Versammlung der Französischen Gemeinschaftskommission, 2020-2021, Nr. 45/1, S. 32).

B.20.3. In ihrer Stellungnahme Nr. 16/2021 vom 10. Februar 2021 über den Entwurf des Zusammenarbeitsabkommens, das zum Zusammenarbeitsabkommen vom 12. März 2021 geworden ist, hat die Datenschutzbehörde angemerkt:

« 33. Les finalités suivantes formulées de manière large nécessitent (toujours) au moins d'être davantage délimitées et précisées :

- *‘ la prestation de soins de santé et de traitements, telle que visée à l'article 9, 2, h du RGPD ’,*

- *‘ l'exécution du suivi et de la surveillance post-autorisation des vaccins conformément aux bonnes pratiques recommandées par l'Organisation mondiale de la Santé ’,*

- *‘ l'exécution d'études scientifiques ou statistiques ’,*

- ainsi que la nouvelle finalité apparue dans le projet d'accord de coopération *‘ l'information et la sensibilisation des utilisateurs de soins concernant la vaccination contre la COVID-19 par les prestataires de soins ’.*

34. Conformément à la remarque de l'Autorité dans son avis n° 138/2020 (point 34), les finalités *‘ la pharmacovigilance des vaccins contre la COVID-19 ’* et *‘ la traçabilité des vaccins contre la COVID-19 ’* sont complétées par la réglementation en vigueur en la matière. L'Autorité en prend acte.

35. En vertu de l'article 4, § 2, 4° et 5° du projet d'accord de coopération, les données enregistrées dans Vaccinnet (dont une proportion importante de données de santé sensibles) doivent également permettre de planifier des plages de vaccination ainsi que l'organisation logistique de la vaccination contre la COVID-19. L'Autorité ne peut toutefois pas se défaire de l'impression que la *‘ base de données des codes de vaccination ’* (qui ne contiendra pratiquement aucune donnée de santé sensible (hormis l'état de vaccination)) créée par le projet d'accord de coopération avait précisément pour finalité de couvrir le volet organisationnel et logistique de planification de plages de vaccination et d'invitation à des plages de vaccination (comme il ressort d'ailleurs de l'article 4, § 1er, 1° et 2° du projet d'accord de coopération). Qu'en est-il ? La double mention (article 4, § 1er, 1° et § 2, 4°) d'une finalité (quasi

textuellement) identique (gestion des schémas de vaccination et planification des plages de vaccination) résulte peut-être d'une erreur ?

36. Dans l'avis n° 138/2020, l'Autorité constatait (au point 35) que ' la détermination du taux de vaccination contre la COVID-19 ' semblait être une finalité statistique qui pouvait être réalisée à l'aide de données anonymes (ou au moins de données à caractère personnel pseudonymisées si une anonymisation ne permettait pas de déterminer le taux de vaccination). L'Autorité recommandait dès lors au demandeur de l'ajouter explicitement dans le projet. L'Autorité constate à cet égard que le mot ' anonyme ' a uniquement été ajouté dans l'Exposé des motifs; elle insiste néanmoins (par analogie avec d'autres finalités qui peuvent être réalisées à l'aide de données anonymes/à tout le moins pseudonymisées) pour que ce terme soit repris dans le texte proprement dit du projet d'accord de coopération.

37. Suite à la demande en ce sens de l'Autorité dans l'avis n° 138/2020 (point 36), l'article 4, § 2, 7° du projet d'accord de coopération complète la finalité de ' l'organisation du suivi des contacts ' par un renvoi explicite à ' en exécution de l'Accord de coopération du 25 août 2020 (...) '.

Dans l'Exposé des motifs, l'importance du rapport avec le suivi des contacts est expliquée à l'aide des scénarios suivants :

- ' l'avis qui doit être formulé par le centre de contact peut varier en fonction du fait qu'une personne a ou non été vaccinée;
- la source est vaccinée mais a infecté plusieurs contacts; il s'agit d'un cas d'échec du vaccin ou d'un variant de la souche contre lequel le vaccin n'offre pas de protection et donc d'informations très importantes pour la santé publique;
- la source n'est pas vaccinée, ce qui a causé l'infection d'autres personnes;
- les contacts sont susceptibles d'être vaccinés, ce qui permet à l'épidémie de s'éteindre;
- les contacts ne sont pas vaccinés, il y a donc lieu de continuer à cartographier activement l'épidémie '.

38. L'Autorité prend acte de cette explication et comprend la plus-value des informations relatives à l'état de vaccination pour le suivi des contacts. Elle estime néanmoins indiqué de préciser dans le projet d'accord de coopération quelles données seront par conséquent exportées depuis Vaccinnet vers la (les) Base(s) de données de Sciensano, et au moins d'apporter les modifications nécessaires aux dispositions de l'Accord de coopération du 25 août 2020 où sont décrites les catégories de données de la (des) Base(s) de données qui y est (sont) encadrée(s) et leurs sources. Une éventuelle délibération du Comité de sécurité de l'information concernant un tel flux de données doit en effet correspondre à ce que prescrit sur ce plan la réglementation en la matière, notamment le présent projet d'accord de coopération et davantage encore, l'Accord de coopération du 25 août 2020.

39. L'article 4, § 2, 10° du projet d'accord de coopération mentionne que des études scientifiques ou statistiques seront réalisées ' conformément au titre 4 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel '. L'Autorité fait observer que le titre 4 de la LTD exécute l'article 89, §§ 2

et 3 du RGPD et définit par conséquent le régime d'exception pour des recherches qui ne peuvent être réalisées qu'avec des limitations / dérogations aux droits des personnes concernées, tels que mentionnés aux articles 15 et suivants du RGPD. Qu'en est-il ?

40. À l'article 4, § 2, 11° du projet d'accord de coopération apparaît pour la première fois une nouvelle finalité à atteindre – grâce à l'enregistrement des vaccinations dans Vaccinnet -, à savoir ' l'information et la sensibilisation des utilisateurs de soins concernant la vaccination contre la COVID-19 par les prestataires de soins '. L'Autorité ne voit pas du tout clairement dans quelle mesure la réalisation d'une finalité telle que ' l'information et la sensibilisation à la vaccination contre la COVID-19 ' nécessite des données à caractère personnel. Si le but est une information et une sensibilisation ' personnalisées ' des citoyens qui refusent un vaccin, cela devrait être clairement énoncé dans le projet d'accord de coopération, afin que les parlements concernés puissent l'accepter ou non en connaissance de cause. L'Autorité considère que des campagnes de sensibilisation (de certains groupes cibles) à grande échelle peuvent parfaitement s'effectuer au moyen de données anonymes ».

B.20.4. Der Minister der Volksgesundheit hat präzisiert, dass « das Zusammenarbeitsabkommen nur die Impfkampagne gegen COVID-19 betrifft und dass die Daten nicht für andere Zwecke verwendet werden dürfen » als die Zwecke, die « ausschließlich die Impfkampagne betreffen » (*Parl. Dok.*, Kammer, 2020-2021, DOC 55-1853/002, S. 12).

B.21.1. 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.21.2. Wie in B.16.4 erwähnt, schließt das Recht auf Achtung des Privatlebens den Schutz personenbezogener Daten und persönlicher Informationen ein, zu denen insbesondere Name und Gesundheitsdaten gehören.

Die angefochtenen Akte, die Bestimmungen billigen, die die Verarbeitung personenbezogener Daten, einschließlich sensibler Daten über die Gesundheit, in der Datenbank « Vaccinnet » vorsehen, haben eine Einmischung in das Recht auf den Schutz personenbezogener Daten, das durch die in B.16 zitierten Bestimmungen garantiert wird, zur Folge.

Artikel 4 Absatz 15 der DSGVO definiert « Gesundheitsdaten » als « 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 ». Da sich die in der Datenbank

« Vaccinnet » erfassten Daten insbesondere auf Daten über die Gesundheit im Sinne der vorerwähnten Bestimmung beziehen, müssen sie gemäß Artikel 9 der DSGVO verarbeitet werden.

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.

Im Erwägungsgrund 54 der DSGVO heißt es diesbezüglich:

« Aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit kann es notwendig sein, besondere Kategorien personenbezogener Daten auch ohne Einwilligung der betroffenen Person zu verarbeiten. Diese Verarbeitung sollte angemessenen und besonderen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen unterliegen. In diesem Zusammenhang sollte der Begriff ‘ öffentliche Gesundheit ’ im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates ausgelegt werden und alle Elemente im Zusammenhang mit der Gesundheit wie den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von Gesundheitsversorgungsleistungen und den allgemeinen Zugang zu diesen Leistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen. Eine solche Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber oder Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten ».

B.21.3. 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).

Wie in B.16.9 und B.16.10 erwähnt, muss aufgrund des Legalitätsprinzips jede Person ein ausreichend klares Bild von den Zwecken der Verarbeitung der sie betreffenden Daten haben.

B.22.1. Die angefochtenen Akte verfolgen das legitime Ziel, die Ausbreitung des Coronavirus SARS-CoV-2, das ein über die Luft übertragenes, sehr ansteckendes Virus ist, zu bekämpfen. Die COVID-19-Pandemie ist durch eine hohe Reproduktionszahl gekennzeichnet. Ohne Hygienemaßnahmen kommt es zu einer sehr schnellen exponentiellen Ausbreitung.

Wie in B.2 erwähnt, erfolgt die Registrierung der Impfdaten einerseits im Rahmen der belgischen Impfstrategie, die auf der Grundlage wissenschaftlicher Daten im Bereich der Impfstoffe gegen COVID-19, wie sie zum Zeitpunkt der Annahme der angefochtenen Akte verfügbar waren, erstellt wurde, um die COVID-19-Pandemie durch die Senkung der mit dem Coronavirus COVID-19 verbundenen Ansteckungen zu bekämpfen, sowie andererseits im Rahmen der Umsetzung eines digitalen EU-COVID-Zertifikats auf europäischer Ebene, das auf dem Bestreben der Interoperabilität unter anderem der Impfcertifikate beruht.

In diesem Kontext ist die Registrierung der Impfdaten für die Verfolgung dieser Ziele unerlässlich und die Zentralisierung der Registrierung dieser Daten ermöglicht « die Bestimmung des geeigneten Dosierungsschemas, einschließlich der verschiedenen zu verabreichenden Dosen eines Impfstoffs (korrektes Intervall im Falle eines Mehrfachdosis-Impfstoffs), und soll das reibungslose Funktionieren der Massenimpfkampagne gegen COVID-19 sicherstellen » (*Parl. Dok.*, Wallonisches Parlament, 2020-2021, Nr. 509/1, S. 3).

Eine solche Maßnahme soll deshalb die Gesundheit anderer Personen und die öffentliche Gesundheit sowie die Rechte und Freiheiten anderer Personen garantieren.

B.22.2. In dem Zusammenarbeitsabkommen vom 12. März 2021 sind in diesem Kontext ausdrücklich elf Zwecke festgelegt, für die die in Artikel 3 § 2 erwähnten personenbezogenen Daten erhoben und in der Datenbank « Vaccinnet » verarbeitet werden und in den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 12. März 2021 ist ausdrücklich präzisiert, dass diese Daten « nicht für andere als die in diesem Abkommen vorgesehenen Zwecke verwendet werden [dürfen] », « und insbesondere nicht - aber nicht ausschließlich - zu polizeilichen, kommerziellen, steuerrechtlichen, strafrechtlichen oder staatsicherheitlichen Zwecken » (*Belgisches Staatsblatt* vom 12. April 2021, S. 32407).

Mit der Annahme der angefochtenen Akte haben die verschiedenen zuständigen Gesetzgeber selbst die wesentlichen Elemente der Verarbeitung personenbezogener Daten gemäß dem in B.16.9 und B.16.10 Erwähnten geregelt, indem sie die Verarbeitungszwecke der in die Datenbank « Vaccinnet » aufgenommenen Daten abschließend festgelegt haben.

Außerdem enthalten die allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 12. März 2021 zahlreiche Präzisierungen zu den Zwecken, mit denen auf die Kritik reagiert wurde, die von der Datenschutzbehörde in ihrer in B.20.3 zitierten Stellungnahme geäußert wurde.

B.23.1. Um zu prüfen, ob die in Artikel 4 § 2 des Zusammenarbeitsabkommens erwähnten Zwecke ausreichend festgelegt sind, muss der Gerichtshof in dem in B.2 angeführten Kontext die sich von Natur aus weiter entwickelnde Beschaffenheit des wissenschaftlichen Kenntnisstandes über die Besonderheiten des Coronavirus SARS-CoV-2 und seiner möglichen Mutationen, aber auch die Wirksamkeit der kurze Zeit vor dem Beginn der Impfkampagne auf den Markt gebrachten Impfstoffe und ihre mittel- und langfristige Wirksamkeit berücksichtigen.

B.23.2.1. Aus den in B.20 zitierten Vorarbeiten geht hervor, dass die elf in Artikel 4 § 2 festgelegten Zwecke im direkten Zusammenhang mit der Massenimpfkampagne auf landesweiter Ebene, die auf der Grundlage des wissenschaftlichen Kenntnisstandes zum Zeitpunkt des Beginns dieser Kampagne durchgeführt wurde, stehen.

Aus dem bloßen Umstand, dass es sich um elf Zwecke einer Datenverarbeitung handelt, kann nicht, wie es die klagende Partei anführt, geschlossen werden, dass diese Zwecke an sich

übermäßig wären. Die festgelegte Beschaffenheit eines Zwecks muss nämlich nach den Umständen des Einzelfalls beurteilt werden und die Erläuterung der verschiedenen Zwecke kann eine Garantie für die Datenverarbeitung darstellen (Stellungnahme 03/2013 über Zweckbindung, 2. April 2013, « Artikel 29 »-Datenschutzgruppe, S. 15).

B.23.2.2. Daher sind die Zwecke der « Pharmakovigilanz » (Nr. 2), « Rückverfolgbarkeit von Impfstoffen » (Nr. 3), « Verwaltung der Impfschemas » (Nr. 4), « logistische Organisation der Impfung gegen COVID-19 » (Nr. 5), « Ermittlung der anonymen Durchimpfungsrate der Bevölkerung gegen COVID-19 » (Nr. 6) und « Durchführung der Überwachung und Kontrolle der Impfstoffe nach der Zulassung » (Nr. 8) präzise und direkt mit der Organisation der Massenimpfkampagne gegen COVID-19 auf landesweiter Ebene verbunden.

Diese verschiedenen Elemente sind nämlich notwendig, um die logistische Organisation der Impfung unter Berücksichtigung der verschiedenen einzuladenden Zielgruppen und der Anzahl der zu verabreichenden Dosen zu regeln, aber auch um die Rate der Impfabdeckung und die Fähigkeit des Impfstoffs, eine Immunantwort auszulösen, zu evaluieren und um eventuelle Nebenwirkungen dieses Impfstoffs zu entdecken. Die Überwachung und Kontrolle der Impfungen nach der Zulassung werden gemäß der guten Praxis der Weltgesundheitsorganisation auf diesem Gebiet geregelt. Im Rahmen des Zwecks der « Pharmakovigilanz » sieht Artikel 45 des Gesetzes vom 13. Juni 2021 « zur Festlegung von Maßnahmen zur Bewältigung der COVID-19-Pandemie und anderer dringender Maßnahmen im Bereich der Gesundheitspflege » die Integration der in « Vaccinnet » aufgenommenen Daten in eine föderale Datenbank vor, für die die Föderalagentur für Arzneimittel und Gesundheitsprodukte die Verantwortliche für die Verarbeitung ist.

Entgegen den Ausführungen der klagenden Partei wurde der Zweck in Bezug auf die « Gesundheitspflege- und Behandlungsleistungen » in Artikel 4 § 2 Nr. 1 des Zusammenarbeitsabkommens vom 12. März 2021 unter Verweis auf Artikel 9 Absatz 2 Buchstabe h der DSGVO ausdrücklich beschränkt auf das, was « ausschließlich durch die Impfung und die Maßnahmen zur Unterstützung, Information und Sensibilisierung der Bürger im Zusammenhang mit der Impfung » bezweckt wird. Es wurde auch präzisiert, dass dieser Zweck nicht beinhaltet, « den Zugang zu einer qualitativ hochwertigen Versorgung in irgendeiner Weise aufgrund des Impfstatus einer Person zu beschränken oder mit Bedingungen zu verbinden » (allgemeine Erläuterungen zum Zusammenarbeitsabkommen vom 12. März

2021, *Belgisches Staatsblatt* vom 12. April 2021, S. 32407). Daraus ergibt sich, dass dieser Zweck ebenfalls präzise und direkt mit der Impfung gegen COVID-19 und der medizinischen Überwachung der geimpften Person verbunden ist.

Der in Artikel 4 § 2 Nr. 1 erwähnte Zweck steht daher ebenfalls mit dem in Artikel 4 § 2 Nr. 10 erwähnten Zweck der « Durchführung wissenschaftlicher oder statistischer Studien » sowie mit dem in Artikel 4 § 2 Nr. 11 erwähnten Zweck der « Information und Sensibilisierung von Personen bezüglich der Impfung gegen COVID-19 » im Zusammenhang. Aus den im Bereich der Impfstrategie beschlossenen Grundsätzen geht nämlich hervor, dass Belgien anstrebt, eine Form der Herdenimmunität durch eine ausreichende Impfquote von 70 % der Bevölkerung zu erreichen. Auf die Datenverarbeitung zu wissenschaftlichen und statistischen Zwecken bezieht sich insbesondere Artikel 89 Absatz 1 der DSGVO, der den Grundsatz der Datenminimierung, insbesondere der Pseudonymisierung, vorsieht, die in Artikel 4 § 2 Nr. 10 zumindest vorgesehen ist, falls eine Anonymisierung die Durchführung der wissenschaftlichen oder statistischen Studie nicht ermöglichen würde. Diesbezüglich wurde betont, dass eine « hohe Impfabdeckung in der Bevölkerung angesichts der beispiellosen Krise der COVID-19-Pandemie und auf Ebene des Einzelnen, der in der Lage sein muss, eine informierte Entscheidung für seine persönliche Gesundheit zu treffen, eine unabdingbare und grundlegende Voraussetzung für die öffentliche Gesundheit ist » (allgemeine Erläuterungen zum Zusammenarbeitsabkommen vom 12. März 2021, *Belgisches Staatsblatt* vom 12. April 2021, S. 32407), sodass statistische Studien über diese Impfabdeckung erforderlich sind. Studien über die Impfabdeckung ermöglichen es, den Prozentsatz an geimpften Personen in den spezifischen Risikogruppen zu schätzen, und helfen dabei, eventuelle Lücken des Impfprogramms einzuschätzen, die geschlossen werden müssten, gegebenenfalls durch eine gezielte Information und Sensibilisierung über allgemeine Kampagnen oder auf individueller Ebene je nach den in der Bevölkerung festgestellten Einstellungen. Der Umstand, dass die Impfung auf freiwilliger Basis erfolgt, macht in diesem Kontext den Zweck der Information und Sensibilisierung im Hinblick auf das Ziel, eine ausreichende Impfabdeckung zu erreichen, erforderlich. Auf der Grundlage dieser Kenntnisse kann diese Rolle des Arztes bei dieser gezielten Information wichtig sein, auch wenn es verboten ist, Personen zu kontaktieren, die ausdrücklich angegeben haben, dass sie die Impfung ablehnen (ebenda).

B.23.2.3. Der Zweck in Bezug auf die « Kontaktrückverfolgung » (Nr. 7) hängt mit dem Umstand zusammen, dass sich – bei dem ausschließlichen Zweck der Ermittlung infektiöser

Kontakte – der Impfstatus direkt auf die Ansteckungsgefahr auswirkt. Die Daten, die in diesem Rahmen von « Vaccinnet » an die Datenbank von Sciensano übermittelt werden, sind begrenzt, aber « eine Flexibilität entsprechend den neuesten wissenschaftlichen Erkenntnissen über die Auswirkungen der Impfung auf das Infektionsrisiko [ist] erforderlich » (ebenda, S. 32406).

B.23.2.4. Der Zweck in Bezug auf die « Berechnung der Aufteilung der Impfkosten » (Nr. 9) zwischen dem Föderalstaat und den föderierten Teilgebieten hängt mit dem Umstand zusammen, dass die kostenlose Impfkampagne über ein Zusammenarbeitsabkommen der zuständigen Behörden geregelt wurde und dass die Parteien dieses Abkommens diese Impfung finanzieren müssen.

Der Umstand, dass, wie es die Gesetzgebungsabteilung des Staatsrates betont, die Daten, nicht anonymisiert, sondern nur pseudonymisiert werden können, kann damit gerechtfertigt werden – wie es in den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen zum Grad anonymer Impfungen gegen COVID-19 heißt –, dass die Anonymisierung es womöglich nicht ermöglicht, das angestrebte Ziel zu erreichen (ebenda, S. 32407), aber Artikel 4 § 2 Nr. 8 gewährleistet, dass die betreffenden Daten zumindest pseudonymisiert werden. Auf der Grundlage dieses Zwecks wurden durch das zwischen der Föderalregierung und den in den Artikeln 128, 130 und 135 der Verfassung erwähnten Behörden abgeschlossene Vereinbarungsprotokoll vom 9. Februar 2022 « bezüglich der Kofinanzierung des Impfprogramms gegen COVID-19 » die Kosten der Impfung gegen COVID-19 unter den verschiedenen Behörden aufgeteilt.

In Bezug auf die Anonymisierung oder Pseudonymisierung ist festzustellen, dass es sich dabei um technische und organisatorische Maßnahmen handelt, die zu ergreifen sind, um die Verarbeitung personenbezogener Daten zu schützen, die aber alle beide gewährleisten, dass die Identität der betroffenen Person nicht offengelegt wird. Bestimmte Elemente müssen nämlich « granular » bestimmbar sein – in den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 12. März 2021 wird diesbezüglich das Beispiel genannt, dass in Wohnpflegezentren zwischen dem Pflegepersonal und den Bewohnern unterschieden werden muss (ebenda, S. 32407). Die Entwicklung der Umstände und der tatsächlichen epidemiologischen Situation muss nämlich womöglich eher durch eine Maßnahme als durch eine andere ausgeglichen werden, ohne dass deshalb die Möglichkeit, auf eine von zwei

Maßnahmen zurückzugreifen, als fehlende Festlegung eines wesentlichen Elements der Verarbeitungszwecke der Daten angesehen werden kann.

B.23.3. Aus dem Vorstehenden ergibt sich, dass die in Artikel 4 § 2 des Zusammenarbeitsabkommens definierten Zwecke im direkten Zusammenhang mit der Massenimpfkampagne auf landesweiter Ebene stehen, ausreichend präzise und festgelegt sind und auf das absolut Notwendige im Zusammenhang mit dieser Impfung beschränkt sind.

B.24. Der erste Teil des einzigen Klagegrunds, insofern er gegen die angefochtenen Akte gerichtet ist, insoweit damit Artikel 4 § 2 des Zusammenarbeitsabkommens gebilligt wird, ist unbegründet.

II. In Bezug auf die in Artikel 5 erwähnte, dem Informationssicherheitsausschuss erteilte Ermächtigung, die Mitteilung von personenbezogenen Daten an Dritte zu genehmigen (erster Teil)

B.25.1. Im ersten Teil des Klagegrunds vertritt die klagende Partei die Auffassung, dass die Kategorien von Empfängern der personenbezogenen Daten, die in Artikel 5 des Zusammenarbeitsabkommens vom 12. März 2021 festgelegt sind, keine ausreichenden Garantien für die Vorhersehbarkeit aufweisen. Zudem werde durch Artikel 5 Absatz 3 des Zusammenarbeitsabkommens vom 12. März 2021 dem Informationssicherheitsausschuss die Befugnis übertragen, wesentliche Elemente festzulegen, das heißt Drittstellen, die die erhobenen Daten verarbeiten dürfen, sowie die Verarbeitungszwecke dieser Daten.

B.25.2. Wie in B.10.1 erwähnt, betreffen die Beschwerdegründe der klagenden Partei nur die Datenbank « Vaccinnet », sodass der Gerichtshof den gegen Artikel 5 des Zusammenarbeitsabkommens vom 12. März 2021 gerichteten Klagegrund nur insoweit prüft, als er die Übermittlung der in Artikel 3 § 2 des vorerwähnten Zusammenarbeitsabkommens erwähnten und in der Datenbank « Vaccinnet » gespeicherten Daten betrifft.

B.26.1. Artikel 5 des Zusammenarbeitsabkommens vom 12. März 2021 bestimmt:

« Mit dem alleinigen Ziel, die in Artikel 4 aufgeführten Zwecke zu verwirklichen, dürfen die in Artikel 3 erwähnten personenbezogenen Daten an Personen oder Einrichtungen übermittelt werden, die durch oder aufgrund eines Gesetzes, eines Dekrets oder einer Ordonnanz mit einem Auftrag öffentlichen Interesses beauftragt sind, sofern diese Übermittlung für die Ausführung des Auftrags öffentlichen Interesses der betreffenden Personen oder Einrichtungen erforderlich ist und nur die Daten übermittelt werden, die für die Zwecke von Artikel 4 relevant sind.

Die in Artikel 3 erwähnten personenbezogenen Daten werden an Forschungseinrichtungen übermittelt, wenn sie für die Durchführung wissenschaftlicher oder statistischer Studien erforderlich sind, und zwar nach Anonymisierung der Daten oder zumindest Pseudonymisierung der Daten, falls eine Anonymisierung die Durchführung der wissenschaftlichen oder statistischen Studie nicht ermöglichen würde.

Im Hinblick auf die Überprüfung der Einhaltung der in vorliegendem Artikel festgelegten Bedingungen ist jede Übermittlung von Daten Gegenstand eines Beschlusses der Kammer ‘ Soziale Sicherheit und Gesundheit ’ des Informationssicherheitsausschusses.

Der Informationssicherheitsausschuss veröffentlicht auf dem eHealth-Portal eine genaue Funktionsbeschreibung der Informationssysteme, die zur Umsetzung des vorliegenden Zusammenarbeitsabkommens eingerichtet wurden, und der Informationsflüsse zwischen diesen Informationssystemen, die Gegenstand eines Beschlusses durch den Informationssicherheitsausschuss waren, insbesondere was die Datenverarbeitung, die Verfahren und die Datenbanken betrifft.

Die Beschlüsse des Informationssicherheitsausschusses werden systematisch auf der Website der eHealth-Plattform veröffentlicht ».

B.26.2. Bezüglich der in Artikel 5 erwähnten Übermittlung von Daten an Dritte heißt es in den allgemeinen Erläuterungen des Zusammenarbeitsabkommens vom 12. März 2021:

« Ausschließlich zur Erfüllung der in Artikel 4 erwähnten Zwecke dürfen die in Artikel 3 erwähnten personenbezogenen Daten an Personen oder Einrichtungen übermittelt werden, die durch oder aufgrund eines Gesetzes, eines Dekrets oder einer Ordonnanz mit einem Auftrag öffentlichen Interesses betraut sind, sofern diese Übermittlung für die Ausführung des Auftrags öffentlichen Interesses der betreffenden Personen oder Einrichtungen erforderlich ist und nur die für die in Artikel 4 erwähnten Zwecke relevanten Daten übermittelt werden.

Die in Artikel 3 erwähnten personenbezogenen Daten werden nach Anonymisierung oder zumindest Pseudonymisierung an Forschungseinrichtungen übermittelt, wenn sie für die Durchführung wissenschaftlicher oder statistischer Studien erforderlich sind (Terminologie von Artikel 89 der Datenschutz-Grundverordnung).

Jede Datenübermittlung ist Gegenstand eines Beschlusses der Kammer ‘ Soziale Sicherheit und Gesundheit ’ des Informationssicherheitsausschusses, um die Einhaltung der in diesem Artikel festgelegten Bedingungen zu überprüfen.

Der Informationssicherheitsausschuss kann nur einen Beschluss über den konkreten Datenaustausch im Rahmen des vorliegenden Zusammenarbeitsabkommens fassen und kann daher nicht selbst andere Verarbeitungszwecke oder Kategorien personenbezogener Daten festlegen. Er ist unter keinen Umständen befugt, ein wesentliches Element der Verarbeitung personenbezogener Daten zu bestimmen, gemäß dem in Artikel 22 der Verfassung verankerten Legalitätsprinzip. Er ist daher auf der Grundlage des vorliegenden Zusammenarbeitsabkommens nicht mit einem solchen Auftrag betraut.

Der Informationssicherheitsausschuss veröffentlicht auf dem eHealth-Portal eine genaue Funktionsbeschreibung der Informationssysteme, die zur Umsetzung des vorliegenden Abkommens eingerichtet wurden, und der Informationsflüsse zwischen diesen Informationssystemen, die Gegenstand eines Beschlusses durch den Informationssicherheitsausschuss waren, insbesondere in Bezug auf die Verarbeitung von Informationen, die Verfahren und die Datenbanken.

Zudem werden die Beschlüsse des Informationssicherheitsausschusses systematisch auf der Website der eHealth-Plattform veröffentlicht. Die Beschlüsse des Informationssicherheitsausschusses umfassen stets die verschiedenen Aspekte, die zur Beurteilung der Einhaltung der Vorschriften in Bezug auf den Schutz des Privatlebens bei der Verarbeitung personenbezogener Daten (insbesondere der Datenschutz-Grundverordnung) notwendig sind. So werden die betreffenden Parteien (die für die Verarbeitung Verantwortlichen) immer ausdrücklich vermerkt, wie auch die anvisierten Zwecke und eine (in der Regel erschöpfende) Übersicht über die zu diesen Zwecken zu verarbeitenden personenbezogenen Daten. Der Informationssicherheitsausschuss überprüft insbesondere, ob die Verarbeitung personenbezogener Daten rechtmäßig ist (und somit eine der in Artikel 6 der DSGVO erwähnten Bedingungen erfüllt) und ob die Grundprinzipien (Zweckbindung, Datenminimierung, Beschränkung der Speicherung und Informationssicherheit) eingehalten werden.

Die Verwendung einer gemeinsamen Datenbank schließt nicht aus, dass verschiedene Endbenutzerschnittstellen, möglicherweise spezifisch für ein föderiertes Teilgebiet, zur Einspeisung oder Abfrage der gemeinsamen Datenbank verwendet werden.

Es ist unerlässlich zu präzisieren, dass die auf der Grundlage des vorliegenden Zusammenarbeitsabkommens erhobenen Daten nur in zwei streng begrenzten Fällen übermittelt werden dürfen:

- entweder ist der Dritte kumulativ mit einem Auftrag öffentlichen Interesses betraut und zur Verarbeitung dieser Daten durch oder aufgrund eines Gesetzes, eines Dekrets oder einer Ordonnanz ermächtigt, das/die sich speziell auf einen in vorliegendem Abkommen vorgesehenen Zweck bezieht,
- oder der Dritte ist eine Forschungseinrichtung zur Durchführung wissenschaftlicher oder statistischer Studien. In diesem Fall werden nur anonymisierte oder, falls eine Anonymisierung nicht zielführend ist, pseudonymisierte Daten weitergegeben.

Unter ‘Dritte’ versteht man insbesondere Pflegeanbieter, die zum Nutzer des Gesundheitswesens in einem therapeutischen Verhältnis stehen, und Versicherungsträger, natürlich innerhalb der Grenzen ihrer jeweiligen Aufträge.

Auch wenn es weder möglich noch relevant ist, diese Dritten in einem Zusammenarbeitsabkommen zu bestimmen, so ermöglichen es diese Kriterien dennoch, die Kategorien der betreffenden Dritten abzustecken und streng zu begrenzen. Darüber hinaus zielt die Rolle des Informationssicherheitsausschusses darauf ab, einen zusätzlichen Filter einzubauen, um sicherzustellen, dass der Datenfluss mit dem verfolgten Ziel und dem Wunsch, die Übermittlung der Daten so weit wie möglich zu begrenzen, übereinstimmt. Auf diese Weise ermöglicht er eine notwendige Flexibilität (indem er zum Beispiel die sich entwickelnden Datenströme nicht einfriert) und kann er die Garantien für den Schutz des Privatlebens durch eine sachliche Kontrolle stärken. Er verhindert nämlich, dass ein automatischer Ablauf erzeugt wird, ohne dass vorher geprüft wird, ob er tatsächlich zulässig ist. Wie die Datenschutzbehörde in ihrer Stellungnahme Nr. 16-2021 vom 18. Februar 2021 unterstreicht, bietet ein Beschluss des Informationssicherheitsausschusses auch einen Mehrwert durch eine nähere Beschreibung der Ausführungsmodalitäten, insbesondere im Hinblick auf die Informationssicherheit und die im Gesetz vorgesehene Verhältnismäßigkeit.

Als Antwort auf das Gutachten 68/844/VR des Staatsrates vom 18. Februar 2021 und aufgrund des Vorangehenden ist darauf hinzuweisen, dass die Tatsache, dass die Übermittlung personenbezogener Daten dem Informationssicherheitsausschuss zur Beschlussfassung vorgelegt werden muss, eine im föderalen Gesetz festgelegte Regel ist und eine absichtliche und standardgemäße Datenschutzmaßnahme im Sinne der Datenschutz-Grundverordnung darstellt. Sie beruht auf den Artikeln 6 Absatz 2 und 9 Absatz 4 der Datenschutz-Grundverordnung.

Tatsächlich enthalten die Beschlüsse des Informationssicherheitsausschusses die Maßnahmen in Bezug auf die Informationssicherheit, die die an der Datenübermittlung Beteiligten einhalten müssen, und eine präventive Überprüfung, ob nicht mehr personenbezogene Daten an die Empfängereinrichtung übermittelt werden, als für die Erfüllung der rechtmäßigen Verarbeitungszwecke unbedingt erforderlich sind.

Beschlüsse des Informationssicherheitsausschusses sind für die am Datenaustausch Beteiligten verbindlich. Andererseits dienen sie dazu, den am Datenaustausch Beteiligten Rechtssicherheit zu bieten, damit ein effektiver und effizienter Datenaustausch nicht unnötig durch einen Mangel an Klarheit über die umzusetzenden Maßnahmen zur Informationssicherheit oder über die Rechtmäßigkeit der Übermittlung personenbezogener Daten beeinträchtigt wird.

Beschlüsse des Informationssicherheitsausschusses betreffen ausschließlich den (elektronischen) Datenaustausch. Der Informationssicherheitsausschuss ist für seine Beschlussfassungen an die Gesetzesbestimmungen über die Zweckbestimmungen der Verarbeitung durch Behörden, die diese Daten empfangen, gebunden. Beschlüsse des Informationssicherheitsausschusses bilden für Einrichtungen, die personenbezogene Daten zu rechtmäßigen Zwecken verarbeiten, nur eine Rechtsgrundlage, um diese Daten anderen Einrichtungen im Rahmen der rechtmäßigen Zwecke, für die die Empfängereinrichtung die personenbezogenen Daten selbst verarbeiten kann, zu übermitteln.

Beschlüsse des Informationssicherheitsausschusses bilden keine Rechtsgrundlage für die erste Erfassung und Verarbeitung personenbezogener Daten durch die übermittelnde Einrichtung. Die Empfängereinrichtung muss die personenbezogenen Daten ebenfalls auf der Grundlage der Rechtsgrundlagen verarbeiten, über die sie verfügt. Folglich kann der Informationssicherheitsausschuss weder den Zweck der ursprünglichen Verarbeitung durch die

übermittelnde Einrichtung ausdehnen noch eine Rechtsgrundlage für die Verarbeitung durch die Empfängereinrichtung schaffen, die nicht durch oder aufgrund des Gesetzes vorgesehen ist. Die Beschlüsse erlauben den Datenaustausch unter Einhaltung der in der Beschlussfassung über den Informationssicherheitsplan beschriebenen Modalitäten und unter Einhaltung des Verhältnismäßigkeitsgrundsatzes, erlegen diesen Austausch aber nicht auf.

Der Informationssicherheitsausschuss ist keine Aufsichtsbehörde im Sinne der Datenschutz-Grundverordnung. Er ist also nicht befugt, die Einhaltung der Regeln zu überwachen, Probleme zu lösen, Streitigkeiten beizulegen oder Beschwerden zu bearbeiten. Für diese Angelegenheiten ist nämlich die Datenschutzbehörde zuständig. Die Datenschutzbehörde kann die Beschlüsse des Informationssicherheitsausschusses jederzeit mit übergeordneten Rechtsnormen vergleichen und den Informationssicherheitsausschuss bei Nichtübereinstimmung auffordern, den betreffenden Beschluss zu den angegebenen Punkten neu zu erwägen.

Der Rückgriff auf den Informationssicherheitsausschuss wird daher von den Parteien des vorliegenden Zusammenarbeitsabkommens nicht als Aufgabe von Zuständigkeiten durch eine Anwendung der Regeln gesehen » (*Belgisches Staatsblatt* vom 12. April 2021, SS. 32408-32411; siehe auch *Parl. Dok.*, Kammer, 2020-2021, DOC 55-1853/001, SS. 13-16).

B.27.1. In ihrem Gutachten zum Vorentwurf des Gesetzes, das zum Gesetz vom 2. April 2021 zur Billigung des Zusammenarbeitsabkommens vom 12. März 2021 geworden ist, hat die Gesetzgebungsabteilung des Staatsrates angemerkt:

« S’agissant de la communication de données à caractère personnel issues des bases de données à des tiers, l’article 5, alinéa 1er, de l’accord de coopération subordonne à l’autorisation préalable du Comité de sécurité de l’information toute communication de données à caractère personnel à ‘ des instances ayant une mission d’intérêt public pour les finalités dont sont chargées ces instances par ou en vertu d’une loi, d’un décret ou d’une ordonnance et pour la communication de ces données après anonymisation ou, à tout le moins, pseudonymisation, à des institutions de recherche pour la réalisation d’études scientifiques ou statistiques ’.

Vu le caractère sensible des données à caractère personnel contenues dans les bases de données, les termes décrivant pareillement les tiers auxquels il pourrait être donné accès aux données apparaissent trop larges. L’accord de coopération sera davantage précisé sur ce point » (*Parl. Dok.*, Kammer, 2020-2021, DOC 55-1853/001, S. 45; siehe auch *Parl. Dok.*, Wallonisches Parlament, 2020-2021, Nr. 509/1, S. 81).

Insoweit es in der Absicht der Verfasser des Zusammenarbeitsabkommens gelegen habe, eine Verordnungsbefugnis der Kammer « Soziale Sicherheit und Gesundheit » des Informationssicherheitsausschusses beizubehalten, verweist die Gesetzgebungsabteilung des Staatsrates auf die Anmerkung, die mit dem Gutachten 67.719 vom 15. Juli 2020 zu einem Vorentwurf, der zum Gesetz 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 » geworden ist, zu den (verordnungsrechtlichen) Befugnissen, die der Kammer « Soziale Sicherheit und Gesundheit » des Informationssicherheitsausschusses übertragen worden waren, formuliert wurde:

« 27. Les articles 11, § 3, et 12, § 1er, de l'accord de coopération prévoient une délégation de pouvoir réglementaire à la chambre ' Sécurité sociale et Santé ' du Comité de sécurité de l'information, en ce qui concerne certains aspects de la réglementation du traitement des données à caractère personnel.

L'attribution d'un pouvoir réglementaire à un organisme public, comme le comité de sécurité de l'information, n'est en principe pas conforme aux principes généraux de droit public en ce qu'il est ainsi porté atteinte au principe de l'unité du pouvoir réglementaire et qu'un contrôle parlementaire direct fait défaut. En outre, les garanties dont est assortie la réglementation classique, telles que celles en matière de publication, de contrôle préventif exercé par le Conseil d'État, section de législation, et de rang précis dans la hiérarchie des normes, sont absentes. Pareilles délégations ne se justifient dès lors que dans la mesure où elles sont très limitées et ont un caractère non politique, en raison de leur portée secondaire ou principalement technique. Les organismes qui doivent appliquer la réglementation concernée doivent être soumis à cet égard tant à un contrôle juridictionnel qu'à un contrôle politique.

Par ailleurs, le Comité de sécurité de l'information est un organisme fédéral et une délégation de pouvoir réglementaire à un tel organisme s'analyse comme un abandon de compétences de la part des entités fédérées qui sont parties à l'accord de coopération.

En conclusion, les délégations visées accordées au Comité de sécurité de l'information doivent être transformées en délégations à un accord de coopération d'exécution, à l'instar de l'article 14, § 9, de l'accord de coopération, pour autant du moins qu'il ne règle aucun nouvel élément essentiel du traitement des données à caractère personnel, mais concrétise tout au plus ce qui découle déjà de l'actuel accord de coopération. Si cela ne s'avère pas possible, cet accord de coopération sera d'abord complété » (ebenda, SS. 52-54; siehe auch *Parl. Dok.*, Flämisches Parlament, 2020-2021, Nr. 708/1, SS. 88-89; *Parl. Dok.*, Wallonisches Parlament, 2020-2021, Nr. 509/1, S. 85; *Parl. Dok.*, Parlament der Deutschsprachigen Gemeinschaft, 2020-2021, Nr. 132/1, SS. 32-33; *Parl. Dok.*, Vereinigte Versammlung der Gemeinsamen Gemeinschaftskommission, 2020-2021, Nr. B-65/1, SS. 17-18; *Parl. Dok.*, Versammlung der Französischen Gemeinschaftskommission, 2020-2021, Nr. 45/1, S. 33).

B.27.2. In ihrer Stellungnahme Nr. 16/2021 vom 10. Februar 2021 zum Vorentwurf des Zusammenarbeitsabkommens, das zum Zusammenarbeitsabkommen vom 12. März 2021 geworden ist, hat die Datenschutzbehörde angemerkt:

« 43. L’Autorité prend certes acte du fait que l’article 5 du projet d’accord de coopération renvoie expressément à son article 4, § 3 (‘ Les données collectées dans le cadre du présent accord de coopération ne peuvent être utilisées à d’autres fins que celles prévues dans le présent accord. ’).

Étant donné que l’Autorité avait déjà constaté dans son avis n° 138/2020 et constate à nouveau dans le présent avis que certaines des finalités mentionnées dans le projet d’accord de coopération sont formulées de manière excessivement large – et de ce fait ne répondent pas à l’exigence qui s’applique en la matière d’être déterminées et explicites (voir l’article 5.1.b) du RGPD) -, le renvoi dans l’article 5 du projet d’accord de coopération à l’article 4, § 3 n’offre pas de garanties suffisantes aux personnes concernées sur le plan de la prévisibilité.

Comme déjà indiqué au point 10 du présent avis, le principe de légalité requiert que toute ingérence dans le droit au respect de la protection des données à caractère personnel soit encadrée par une norme qui soit non seulement nécessaire et proportionnée à l’objectif qu’elle poursuit mais qui soit aussi suffisamment claire et précise et dont l’application est prévisible pour les personnes concernées. Un manque de prévisibilité affecte donc inévitablement aussi la légalité de la norme.

[...]

45. Dans la mesure où le projet d’accord de coopération prévoit un énoncé plus clair des catégories de destinataires visées ainsi qu’une délimitation plus claire des finalités (à quelles fins ces tiers peuvent-ils utiliser les données en question), une délibération du Comité de sécurité de l’information peut évidemment apporter une plus-value en précisant davantage les modalités d’exécution, notamment au niveau de la sécurité de l’information.

L’Autorité insiste à cet égard pour que – outre la description fonctionnelle des systèmes d’information et des flux d’informations qui ont fait l’objet d’une délibération (voir l’article 5, dernier alinéa du projet d’accord de coopération) – les délibérations proprement dites du Comité de sécurité de l’information soient aussi publiées immédiatement et intégralement et qu’elles puissent être consultées pendant une longue période ».

B.27.3. Der Minister der Volksgesundheit hat diesbezüglich präzisiert, dass « die Aufgabe des Informationssicherheitsausschusses strikt abgegrenzt ist. Er kann nur Beschlüsse über die Datenübermittlungen fassen, die im Rahmen dieses Zusammenarbeitsabkommens erfolgen. Dieser Ausschuss kann auf keinen Fall selbst andere Zwecke oder andere Kategorien persönlicher Daten festlegen » (*Parl. Dok.*, Kammer, 2020-2021, DOC 55-1853/002, S. 13).

Die wallonische Ministerin der Gesundheit hat auch präzisiert, dass « nur Dritte, die mit einer Aufgabe des öffentlichen Dienstes betraut sind und die gesetzlich ermächtigt sind, personenbezogene Daten zu verarbeiten, die Daten erhalten dürfen » (*Parl. Dok.*, Wallonisches Parlament, *CRI*, Nr. 25, 2020-2021, 31. März 2021, S. 73).

B.28. Was die in der Datenbank « Vaccinnet » aufgenommenen personenbezogenen Daten betrifft, legt Artikel 5 des Zusammenarbeitsabkommens zwei Kategorien von Dritten fest, an die diese Daten übermittelt werden dürfen: einerseits « Personen oder Einrichtungen [...], die durch oder aufgrund eines Gesetzes, eines Dekrets oder einer Ordonnanz mit einem Auftrag öffentlichen Interesses betraut sind », an die von den in Artikel 3 § 2 erwähnten Daten nur die für die in Artikel 4 § 2 erwähnten Zwecke relevanten Daten übermittelt werden dürfen und nur wenn diese Übermittlung für die Ausführung des Auftrags öffentlichen Interesses dieser Personen oder Einrichtungen erforderlich ist; andererseits « Forschungseinrichtungen », wenn die Daten für die Durchführung wissenschaftlicher oder statistischer Studien erforderlich sind, nach Anonymisierung oder zumindest Pseudonymisierung, falls eine Anonymisierung die Durchführung der wissenschaftlichen oder statistischen Studie nicht ermöglichen würde.

Artikel 5 Absatz 3 knüpft jedoch die Übermittlung dieser personenbezogenen Daten an die Bedingung eines Beschlusses der « Kammer Soziale Sicherheit und Gesundheit » des Informationssicherheitsausschusses, um die Einhaltung der in diesem Artikel festgelegten Bedingungen zu überprüfen.

B.29.1. Wie in B.16.9 und B.16.10 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.29.2. 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 h der DSGVO erlaubt die Verarbeitung sensibler Daten für Zwecke der Gesundheitsvorsorge, versehen mit verschiedenen Garantien, insbesondere dem Berufsgeheimnis. 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.

B.30.1. 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 5 des Zusammenarbeitsabkommens vom 12. März 2021 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 derselben 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 seiner 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.30.2. Aus dem Vorstehenden geht hervor, dass die Beschlüsse des Informationssicherheitsausschusses, wie der Gerichtshof mit seiner Entscheidung Nr. 110/2022 vom 22. September 2022 geurteilt hat (ECLI:BE:GHCC:2022:ARR.110), 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.31. Wie die Gesetzgebungsabteilung des Staatsrates in ihrem Gutachten über den Gesetzesvorentwurf, der zum Gesetz vom 2. April 2021 geworden ist, angemerkt hat, steht eine solche Ermächtigung einer Einrichtung wie des Informationssicherheitsausschusses « grundsätzlich nicht mit den allgemeinen Grundsätzen des öffentlichen Rechts in Einklang, insofern so der Grundsatz der Einheit der Verordnungsbefugnis beeinträchtigt wird und eine direkte parlamentarische Kontrolle fehlt », insofern « die Garantien [...] auf dem Gebiet der Bekanntmachung, der präventiven Prüfung durch die Gesetzgebungsabteilung des Staatsrates und des genauen Rangs in der Normenhierarchie » nicht vorhanden sind (*Parl. Dok.*, Kammer, 2020-2021, DOC 55-1853/001, S. 53). Derartige Ermächtigungen könnten nur gerechtfertigt werden, wenn sie aufgrund ihrer untergeordneten oder hauptsächlich technischen Tragweite sehr begrenzt wären, was im vorliegenden Fall nicht zutrifft. 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, deren Rechtsstellung nicht durch das Gesetz präzisiert ist und deren 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 5 des Zusammenabkommens vom

12. März 2021 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.

B.32. Der erste Teil des einzigen Klagegrunds, insofern er gegen die angefochtenen Akte gerichtet ist, insoweit damit Artikel 5 des Zusammenarbeitsabkommens vom 12. März 2021 gebilligt wird, in dem Maße, in dem dieser Artikel die Übermittlung der in Artikel 3 § 2 des vorerwähnten Zusammenarbeitsabkommens erwähnten und in der Datenbank « Vaccinnet » gespeicherten Daten betrifft, ist begründet.

Die angefochtenen Akte sind in diesem Maße, insoweit damit Artikel 5 des Zusammenarbeitsabkommens vom 12. März 2021 gebilligt wird, für nichtig zu erklären.

III. In Bezug auf die Dauer der Aufbewahrung der in « Vaccinnet » gespeicherten Daten, die in Artikel 6 § 2 erwähnt ist (zweiter Teil)

B.33. Im zweiten Teil des Klagegrunds vertritt die klagende Partei die Auffassung, dass die Dauer der Aufbewahrung der in « Vaccinnet » gespeicherten Daten, die in Artikel 6 § 2 des Zusammenarbeitsabkommens vom 12. März 2021 erwähnt ist, unverhältnismäßig ist, einerseits insofern die Frist von 30 Jahren für die Aufbewahrung der Daten ab dem Datum der Impfung gegen COVID-19 übermäßig ist und andererseits wegen des Fehlens einer Höchstfrist für die Aufbewahrung von Daten.

B.34.1. Artikel 6 § 2 des Zusammenarbeitsabkommens vom 12. März 2021 bestimmt:

« Die in Artikel 3 § 2 erwähnten Daten werden bis zum Tod der Person, der der Impfstoff gegen COVID-19 verabreicht wurde, und mindestens dreißig Jahre ab der Impfung aufbewahrt ».

B.34.2. Bezüglich der in Artikel 6 erwähnten Dauer der Aufbewahrung der Daten heißt es in den allgemeinen Erläuterungen des Zusammenarbeitsabkommens vom 12. März 2021:

« Die Daten zum Impfcodes werden bis fünf Tage, gerechnet ab dem Tag nach dem Tag der Veröffentlichung des Königlichen Erlasses zur Erklärung der Beendigung des Zustands der Epidemie des Coronavirus COVID-19, aufbewahrt. In der Tat ist, solange die Pandemie andauert, eine genaue Nachverfolgung in diesem Zusammenhang notwendig.

Darüber hinaus regelt Artikel 6 die Aufbewahrungsfrist der personenbezogenen Daten von Vaccinnet bis zum Tod der Person, der der Impfstoff gegen COVID-19 verabreicht wurde, und während mindestens dreißig Jahren ab der Impfung.

Neben der Wichtigkeit für den Nutzer des Gesundheitswesens und die Pflegeanbieter, jederzeit ein genaues Bild der verabreichten Impfungen zu haben, ist diese Aufbewahrungsfrist für eine korrekte Nachverfolgung notwendiger Auffrischungen erforderlich, insbesondere bei Impfstoffen, für die die Dauer der Schutzwirkung noch nicht bekannt ist. Im Allgemeinen werden personenbezogene Gesundheitsdaten standardmäßig in der medizinischen Akte während mindestens dreißig Jahren nach dem letzten Kontakt aufbewahrt. Die Aufbewahrungsfrist ermöglicht auch eine Längsschnittüberwachung für wissenschaftliche Forschungszwecke. Schließlich ist diese Aufbewahrungsfrist im Zusammenhang mit den Haftungsregeln für die beteiligten Parteien wichtig, angesichts der Ungewissheit bezüglich möglicher unerwünschter Auswirkungen auf lange Sicht.

Ein Impfstoff soll ein Leben lang wirken. Aus diesem Grund werden viele Impfstoffe bereits in jungen Jahren verabreicht und sind später keine neuen Auffrischungsimpfungen für verschiedene Krankheiten, gegen die geimpft wird, erforderlich. Daher ist es wichtig, auch nach dreißig Jahren zu wissen, ob jemand einen bestimmten Impfstoff erhalten hat. Für den Arzt, aber auch für den Geimpften ist es wichtig, den Impfstatus von Impfstoffen, die vor längerer Zeit verabreicht wurden, zu kennen.

Bei der wissenschaftlichen Überwachung der Wirksamkeit von Impfstoffen ist es jedoch auch notwendig, noch nach mehr als dreißig Jahren zu überprüfen, ob jemand geimpft worden ist. So hat man zum Beispiel festgestellt, dass der Impfstoff gegen Keuchhusten bei älteren Menschen an Kraft verliert, sodass eine Auffrischungsimpfung vorgenommen wird. Um diese Studien durchführen zu können, muss man natürlich wissen, ob eine Impfung erfolgt ist.

Nebenwirkungen von Medikamenten, zu denen die Impfstoffe gehören, treten manchmal erst nach vielen Jahren auf. Ein klassisches Beispiel für ein Medikament ist Diethylstilbestrol (DES), ein Hormon, das Frauen verabreicht wird. Bei zahlreichen Mädchen, die von DES-Müttern geboren wurden, hat man ein erhöhtes Risiko für Vaginal- und Gebärmutterhalskrebs im Erwachsenenalter festgestellt. Wären diese Daten vernichtet worden, hätte man diese Verbindung vielleicht nicht herstellen können. Verzögerte Effekte können aber auch positiv sein. So gibt es zum Beispiel die Hypothese, dass Personen (zum Beispiel Kinder), denen vor langer Zeit ein BCG-Tuberkulose-Impfstoff verabreicht wurde, weniger empfindlich auf COVID-19 reagieren könnten.

Schließlich darf ein begrenzter Satz von Daten, die mit Laborergebnissen aus der Datenbank I des Zusammenarbeitsabkommens vom 25. August 2020 verknüpft sind, nicht nach sechzig Tagen gelöscht werden. Diese Daten sind in der Tat für die operationellen Abläufe und Zwecke im Zusammenhang mit der Registrierung von Impfungen erforderlich. Dies betrifft zunächst den Zweck der Pharmakovigilanz. Zu diesem Zweck kann im Rahmen sogenannter ‘ Durchbruchsfälle ’, bei denen sich eine geimpfte Person dennoch mit COVID-19 infiziert, das beteiligte Labor aufgefordert werden, eine ‘ Gesamtgenomsequenzierung ’ durchzuführen, um die Ursache des Impfersagens zu untersuchen. Darüber hinaus ist die Speicherung dieser Daten auch während eines längeren Zeitraums zum Zwecke der logistischen Organisation von Impfungen gegen COVID-19 erforderlich. Daten über frühere Infektionen, die bereits zum Erwerb einer gewissen Immunität geführt haben, können in der Tat relevant sein, wenn es

darum geht, die Priorität der Impfung von Zielgruppen zu bestimmen » (*Belgisches Staatsblatt* vom 12. April 2021, SS. 32411-32412; siehe auch *Parl. Dok.*, Kammer, 2020-2021, DOC 55-1853/001, SS. 16-18).

B.35.1. In ihrem Gutachten zum Vorentwurf des Gesetzes, das zum Gesetz vom 2. April 2021 zur Billigung des Zusammenarbeitsabkommens vom 12. März 2021 geworden ist, hat die Gesetzgebungsabteilung des Staatsrates angemerkt:

« 30. Conformément au texte néerlandais de l'article 6, § 2, de l'accord de coopération, les données de la base de données Vaccinnet sont conservées ' gedurende 30 jaar na de vaccinatie tegen COVID-19 of in elk geval tot minstens 1 jaar na het overlijden van de persoon waaraan het vaccin werd toegediend '. Selon le texte français, ces données sont conservées ' pendant 30 ans à compter de la date de vaccination contre la COVID-19 et en tout cas pendant un an au moins après le décès de la personne qui a reçu le vaccin '. Selon le texte allemand, les données sont conservées ' *dreißig Jahre nach dem Datum der Impfung gegen COVID-19 und in jedem Fall mindestens ein Jahr nach dem Tod der Person, der der Impfstoff verabreicht wurde* '.

Indépendamment de la question de savoir si les différentes conjonctions (' of ', ' et ' et ' und ') ne donnent pas une portée différente à cette disposition, le Conseil d'État se demande pourquoi il est prévu un si long délai de trente ans, compte tenu notamment de l'article 5, paragraphe 1, e), du RGPD.

Même s'il peut être admis que le délai d'un an après le décès de la personne vaccinée est dicté par des considérations relatives à la pharmacovigilance, la mention ' au moins ' ne fixe pas de délai maximum, mais un délai minimum de conservation. Sans doute faut-il écrire ' au maximum ' au lieu de ' au moins ' » (ebenda, SS. 54-55; siehe auch *Parl. Dok.*, Flämisches Parlament, 2020-2021, Nr. 708/1, SS. 90; *Parl. Dok.*, Wallonisches Parlament, 2020-2021, Nr. 509/1, SS. 85-86; *Parl. Dok.*, Parlament der Deutschsprachigen Gemeinschaft, 2020-2021, Nr. 132/1, SS. 32-33; *Parl. Dok.*, Vereinigte Versammlung der Gemeinsamen Gemeinschaftskommission, 2020-2021, Nr. B-65/1, SS. 18-19; *Parl. Dok.*, Versammlung der Französischen Gemeinschaftskommission, 2020-2021, Nr. 45/1, SS. 33-34).

B.35.2. In ihrer Stellungnahme Nr. 16/2021 vom 10. Februar 2021 zum Vorentwurf des Zusammenarbeitsabkommens, das zum Zusammenarbeitsabkommen vom 12. März 2021 geworden ist, hat die Datenschutzbehörde angemerkt:

« 51. Les données à caractère personnel enregistrées dans Vaccinnet en application du projet d'accord de coopération sont conservées, en vertu de son article 6, § 2, pendant 30 ans à compter de la date de vaccination contre la COVID-19 et en tout cas pendant un an au moins après le décès de la personne qui a reçu le vaccin.

52. L'Autorité estime que le délai de conservation de 30 ans prévu dans le projet d'accord de coopération peut éventuellement être retenu pour des données pseudonymisées dans le cadre de finalités plutôt scientifiques/statistiques. Pour des finalités plus opérationnelles, ce délai de conservation extrêmement long paraît excessif ».

B.35.3. Zur Dauer der Aufbewahrung der Daten hat die wallonische Ministerin der Gesundheit darauf hingewiesen, dass « die Gültigkeitsdauer des Impfstoffs heute noch nicht bekannt ist » und dass « es wichtig ist, den Impfstatus einer Person auch viele Jahre nach der Impfung zu kennen » (*Parl. Dok.*, Wallonisches Parlament, *CRI*, Nr. 25, 2020-2021, 31. März 2021, S. 74).

B.35.4. Vor der Versammlung der Französischen Gemeinschaftskommission hat der Minister der Gesundheit ebenfalls präzisiert:

« Concernant la base de données Vaccinnet+, le délai de conservation des données est de 30 ans car cette durée préexistait à l'accord de coopération. Cela semble long mais fut jugé nécessaire par les scientifiques. En effet, il est primordial que la personne vaccinée ainsi que les prestataires de soins puissent se faire une idée des vaccinations administrées au fur et à mesure de la vie de cette personne.

Dans le cadre de rappels de vaccins, cela peut également être utile. La durée de protection du vaccin contre la Covid-19 n'est pas encore connue. Il est impossible de savoir, aujourd'hui, ce qui se passera dans six mois, un an, voire deux ans. Il est donc important d'avoir l'opportunité, à cet instant, de consulter les dossiers de vaccination des citoyens afin de savoir, exactement, quels sont les vaccins reçus, dans quels délais, etc.

Pour les études relatives au suivi scientifique de l'efficacité des vaccins, il est également nécessaire de vérifier, bien après 30 ans, si un citoyen est vacciné. Il cite en exemple le vaccin de la coqueluche, qui perd de sa force chez les personnes âgées et qui nécessite un rappel.

Ce délai de conservation est donc important, dans le cadre des règles de responsabilité vis-à-vis des acteurs concernés. Aussi, étant donné l'incertitude relative aux effets indésirables potentiels sur le long terme, bien que ceux-ci soient rares, voire extrêmement rares, il est primordial de pouvoir effectuer des anamnèses de nombreuses années après l'administration d'un vaccin » (*Parl. Dok.*, Versammlung der Französischen Gemeinschaftskommission, 2020-2021, Nr. 45/2, S. 12).

B.36.1. 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.36.2. Artikel 6 § 2 des Zusammenarbeitsabkommens vom 12. März 2021 legt eine Höchstdauer für die Aufbewahrung der Daten fest.

Die in der Datenbank « Vaccinnet » gespeicherten Daten werden mindestens dreißig Jahre und höchstens bis zum Tod der betroffenen Person aufbewahrt.

B.37.1. Die Notwendigkeit der Dauer der Aufbewahrung der Daten wird anhand der Umstände des Einzelfalls und unter Berücksichtigung des Umstands beurteilt, dass die für die Aufbewahrung von Gesundheitsakten und im Rahmen der wissenschaftlichen Forschung im Gesundheitsbereich allgemein akzeptierte Frist relativ lang ist.

B.37.2. Aufgrund von Artikel 9 § 1 des Gesetzes vom 22. August 2002 über die Rechte des Patienten hat der Patient « seitens der Berufsfachkraft ein Recht auf eine sorgfältig fortgeschriebene und an einem sicheren Ort aufbewahrte Patientenakte » und auf seinen Antrag « fügt die Berufsfachkraft die vom Patienten beigebrachten Dokumente der ihn betreffenden Patientenakte bei ».

In den Vorarbeiten zu dieser Bestimmung heißt es:

« L'alinéa 1er de l'article 9, § 1er, dispose que le patient a droit à un dossier de patient soigneusement tenu à jour et conservé en lieu sûr. Les normes auxquelles le dossier de patient doit répondre, entre autres, sur le plan du contenu, ne sont pas réglées par le présent projet. A cet égard, on peut renvoyer entre autres à l'AR du 3 mai 1999 relatif au dossier médical général et à l'AR du 3 mai 1999 portant fixation des normes minimales générales auxquelles le dossier médical, tel que visé à l'article 15 de la loi sur les hôpitaux, doit répondre » (*Parl. Dok.*, Kammer, 2001-2002, DOC 50-1642/001, S. 29).

Artikel 1 des königlichen Erlasses vom 3. Mai 1999 « über die allgemeine medizinische Akte » definiert die « allgemeine medizinische Akte » (AMA) als « eine funktionelle und selektive Sammlung sachdienlicher medizinischer, sozialer und administrativer Daten in bezug auf einen Patienten, die Gegenstand manueller oder computergestützter Verarbeitung sind » und die insbesondere « die Anamnese und die bisherigen medizinischen Daten (Krankheiten, Operationen, erhaltene Impfungen) » umfasst.

Artikel 1 § 3 des königlichen Erlasses vom 3. Mai 1999 « zur Festlegung der allgemeinen Mindestbedingungen, denen die in Artikel 15 des am 7. August 1987 koordinierten Gesetzes über die Krankenhäuser erwähnte medizinische Akte genügen muss » sieht vor, dass die für jeden Patienten in einem Krankenhaus angelegte medizinische Akte « mindestens dreißig Jahre lang im Krankenhaus aufbewahrt werden muss ».

Artikel 35 des Gesetzes vom 22. April 2019 « über die Qualität der Ausübung der Gesundheitspflege » bestimmt:

« Le professionnel des soins de santé conserve le dossier du patient pendant minimum 30 ans et maximum 50 ans à compter du dernier contact avec le patient ».

Artikel 24 des Kodex der ärztlichen Berufspflichten bestimmt:

« Les dossiers des patients doivent être conservés pendant trente ans après le dernier contact avec le patient, de manière sécurisée et en respectant le secret professionnel. Passé ce délai, le médecin peut détruire les dossiers.

Lorsque sa pratique cesse, le médecin transmet au médecin désigné par le patient ou au patient tous les renseignements utiles pour garantir la continuité des soins ».

Aus dem Vorstehenden ergibt sich, dass eine Aufbewahrungsfrist von mindestens 30 Jahren die Frist darstellt, die gewöhnlich im Bereich Gesundheitsdaten akzeptiert wird.

B.37.3. Es sind ebenfalls die Umstände der pandemischen Notsituation bei der Entwicklung, Zulassung, Herstellung und Verabreichung von Impfstoffen gegen COVID-19 und die Notwendigkeit, die mittel- und langfristige Wirksamkeit dieser Impfstoffe ebenso wie ihre eventuellen Nebenwirkungen beurteilen zu können, zu berücksichtigen. Insbesondere wegen dieser Beurteilung wurden die Zwecke im Zusammenhang mit den Gesundheitspflege- und Behandlungsleistungen (Artikel 4 § 2 Nr. 1), der Pharmakovigilanz (Artikel 4 § 2 Nr. 2), der Überwachung und Kontrolle nach der Zulassung der Impfstoffe (Artikel 4 § 2 Nr. 8) oder der Durchführung wissenschaftlicher oder statistischer Studien (Artikel 4 § 2 Nr. 10) festgelegt.

B.37.4. Angesichts des Vorstehenden geht die Aufbewahrung der Daten der Impfung gegen COVID-19 bis zum Tod der geimpften Person nicht über das Notwendige im Hinblick auf die Zwecke, für die sie verarbeitet werden, hinaus.

B.38. Der zweite Teil des einzigen Klagegrunds, insofern er gegen die angefochtenen Akte gerichtet ist, insoweit damit Artikel 6 § 2 des Zusammenarbeitsabkommens gebilligt wird, ist unbegründet.

IV. In Bezug auf das Fehlen einer nach Artikel 35 der DSGVO erforderlichen vorherigen Folgenabschätzung (zweiter Teil)

B.39. Die klagende Partei beanstandet die fehlende Durchführung einer vorherigen Datenschutz-Folgenabschätzung im Sinne von Artikel 35 der DSGVO, sodass aufgrund des Fehlens dieser Folgenanalyse gegen die im Klagegrund erwähnten Bestimmungen verstoßen würde.

B.40. In den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 12. März 2021 heißt es:

« Das Zusammenarbeitsabkommen ist der Datenschutzbehörde zur Stellungnahme (Stellungnahme Nr. 16-2021 vom 10. Februar 2021), der ‘ Vlaamse Toezichtscommissie ’ zur Stellungnahme (Stellungnahme Nr. 2021/13 vom 17. Februar 2021), dem Staatsrat zur Begutachtung (Gutachten Nr. 68.832/VR, Nr. 68.836/VR, Nr. 68.837/VR, Nr. 68.839/VR, Nr. 68.840/VR und Nr. 68.844/VR vom 18. Februar 2021), dem ‘ Vlaamse Raad WVG ’ (Flämischer Rat für Wohlbefinden, Volksgesundheit und Familie) zur Stellungnahme (Stellungnahme vom 16. Februar 2021), im französischsprachigen Konzertierungsorgan zur Stellungnahme und im französischsprachigen ministeriellen Konzertierungsausschuss zur Konzertierung (Stellungnahme vom 15. Februar 2021) vorgelegt worden.

In Anwendung der Artikel 35 und 36 der Datenschutz-Grundverordnung wird eine Datenschutz-Folgenabschätzung erstellt » (*Belgisches Staatsblatt* vom 12. April 2021, S. 32398).

B.41.1. In ihrem Gutachten zum Vorentwurf des Gesetzes, das zum Gesetz vom 2. April 2021 zur Billigung des Zusammenarbeitsabkommens vom 12. März 2021 geworden ist, hat die Gesetzgebungsabteilung des Staatsrates angemerkt:

« À la question de savoir si cette analyse d’impact avait déjà été effectuée, les délégués ont répondu :

‘ *Nee, dit zal nog gebeuren* ’.

L’auteur de l’avant-projet veillera par conséquent au bon accomplissement de cette étude d’impact, si possible avant l’assentiment par l’assemblée législative de l’accord de coopération à l’examen » (*Parl. Dok.*, Kammer, 2020-2021, DOC 55-1853/001, S. 46; siehe auch *Parl. Dok.*, Flämisches Parlament, 2020-2021, Nr. 708/1, S. 82; *Parl. Dok.*, Wallonisches Parlament, 2020-2021, Nr. 509/1, SS. 81-82; *Parl. Dok.*, Parlament der Deutschsprachigen Gemeinschaft,

2020-2021, Nr. 132/1, SS. 27-28; *Parl. Dok.*, Vereinigte Versammlung der Gemeinsamen Gemeinschaftskommission, 2020-2021, Nr. B-65/1, SS. 11-12; *Parl. Dok.*, Versammlung der Französischen Gemeinschaftskommission, 2020-2021, Nr. 45/1, S. 29).

B.41.2. In ihrer Stellungnahme Nr. 16/2021 vom 10. Februar 2021 hat die Datenschutzbehörde, wie sie es bereits in ihrer Stellungnahme Nr. 138/2020 vom 18. Dezember 2020 zum königlichen Erlass vom 24. Dezember 2020 (Nummer 21) getan hatte, angemerkt:

« Étant donné que les enregistrements de données en matière de vaccinations contre la COVID-19 encadrés dans le projet d'accord de coopération s'accompagnent de traitements à grande échelle d'une catégorie particulière de données à caractère personnel, à savoir des données relatives à la santé, le(s) responsable(s) du traitement est (sont) tenu(s), en vertu de l'article 35.3 du RGPD, de réaliser préalablement au traitement une analyse d'impact relative à la protection des données. Bien que l'Autorité ait déjà souligné l'importance de cette disposition dans son avis n° 138/2020, le demandeur indique toujours dans le formulaire de demande d'avis que les traitements visés par le projet d'accord de coopération n'ont pas été soumis à une telle analyse d'impact relative à la protection des données. L'Autorité insiste à nouveau dans le présent avis pour qu'une telle analyse soit réalisée » (Ziffer 19).

B.41.3. In dem Bericht vom 23. März 2021 hat der Minister der Volksgesundheit angegeben:

« L'analyse d'impact relative à la protection des données (*data protection impact assessment*) a été réalisée et un résumé est disponible » (*Parl. Dok.*, Kammer, 2020-2021, DOC 55-1853/002, S. 14).

B.42. Hat die Verarbeitung personenbezogener Daten voraussichtlich « ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen » zur Folge, muss der Verantwortliche gemäß Artikel 35 der DSGVO vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen. Aufgrund von Artikel 36 der DSGVO muss der Verantwortliche, wenn aus der Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, vor der Verarbeitung die Aufsichtsbehörde konsultieren.

B.43. Artikel 35 der DSGVO schreibt die Durchführung einer Datenschutz-Folgenabschätzung vor der materiellen Handlung der Verarbeitung, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, vor, aber nicht vor oder bei der Ausarbeitung einer Gesetzesbestimmung zu einer solchen

Verarbeitung. Da die vorherige Beschaffenheit der Folgenabschätzung eine materielle Verarbeitungshandlung betrifft, fällt sie nicht in die Zuständigkeit des Gerichtshofs, sondern in die Zuständigkeit des ordentlichen oder administrativen Richters.

Diese Feststellung berührt nicht die Verpflichtung der Mitgliedstaaten gemäß Artikel 36 Absatz 4 der DSGVO, « die Aufsichtsbehörde bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regulationsmaßnahmen, die die Verarbeitung betreffen » zu konsultieren, auf die der Gesetzgeber im vorliegenden Fall verwiesen hat.

B.44.1. Schließlich ist die Kritik, die gegen die Vertraulichkeit der Folgenabschätzung gerichtet ist und die von der klagenden Partei in ihrem Erwidernsschriftsatz vorgebracht wird, nicht zulässig, denn damit würde die Tragweite des zweiten Teils des Klagegrunds geändert, der sich darauf beschränkte, die fehlende vorherige Folgenabschätzung zu kritisieren.

Es obliegt nämlich einer klagenden Partei nicht, in ihrem Erwidernsschriftsatz den Klagegrund zu ändern, den sie selbst in der Klageschrift verfasst hat. Ein Beschwerdegrund, der wie im vorliegenden Fall in einem Erwidernsschriftsatz vorgebracht wird, aber von dem abweicht, was in der Klageschrift formuliert worden ist, ist daher ein neuer Klagegrund dar und ist unzulässig.

B.44.2. Im Übrigen verpflichtet die DSGVO nicht zur Veröffentlichung dieser Analyse (Leitlinien für die Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob die Verarbeitung im Sinne der Verordnung (EU) 2016/679 « wahrscheinlich ein hohes Risiko mit sich bringt », 4. April 2017, zuletzt geändert am 4. Oktober 2017, « Artikel 29 »-Datenschutzgruppe, S. 21). Die Vertraulichkeit kann nämlich dadurch gerechtfertigt sein, dass sich die Folgenabschätzung auf etwaige Risiken im Bereich Sicherheit und insbesondere auf die technische Beschreibung der geplanten Maßnahmen, um diese Risiken abzumildern, bezieht. Eine Bekanntmachung dieser Analyse könnte folglich zu einer Gefährdung der Sicherheit der Verarbeitung dieser Daten führen und würde somit das Recht auf Achtung des Privatlebens und auf Schutz der persönlichen Daten gefährden.

B.45. Der zweite Teil des einzigen Klagegrunds, insofern er gegen die angefochtenen Akte gerichtet ist, insoweit ihnen keine vorherige Folgenabschätzung vorangegangen wäre, ist unbegründet.

V. In Bezug auf die Rückwirkung des Zusammenarbeitsabkommens zum 24. Dezember 2020, die in Artikel 12 vorgesehen ist (dritter Teil)

B.46. Im dritten Teil des Klagegrunds vertritt die klagende Partei die Auffassung, dass die angefochtenen Akte im Widerspruch zum Grundsatz der Nichtrückwirkung der Gesetze stehen, der es erfordert, dass der Inhalt des Rechts vorhersehbar und zugänglich ist, damit der Rechtsunterworfenen in einem vernünftigen Maße die Folgen eines bestimmten Handelns zum Zeitpunkt der Ausführung dieser Handlung vorhersehen kann.

So sieht Artikel 12 des Zusammenarbeitsabkommens vom 12. März 2021 vor, dass die Bestimmungen dieses Abkommens rückwirkend zum Tag des Inkrafttretens des königlichen Erlasses vom 24. Dezember 2020 gelten, obgleich - wie die klagende Partei betont - der elfte in Artikel 4 § 2 des Zusammenarbeitsabkommens enthaltene Zweck nicht im königlichen Erlass vom 24. Dezember 2020 aufgeführt war.

B.47.1. Artikel 12 des Zusammenarbeitsabkommens vom 12. März 2021 bestimmt:

« Vorliegendes Zusammenarbeitsabkommen ist wirksam ab dem 24. Dezember 2020, was die Bestimmungen betrifft, deren Inhalt dem des Königlichen Erlasses vom 24. Dezember 2020 über die Registrierung und Verarbeitung von Daten über Impfungen gegen COVID-19 entspricht, und ab dem 11. Februar 2021, was die anderen Bestimmungen betrifft.

Vorliegendes Zusammenarbeitsabkommen ist wirksam bis es an dem Tag abgeändert oder widerrufen wird, an dem das Zentrale Sekretariat des Konzertierungsausschusses die schriftliche Zustimmung aller Parteien zur Beendigung des Zusammenarbeitsabkommens erhalten hat und nachdem eine Mitteilung, in der diese schriftliche Zustimmung bestätigt wird, im *Belgischen Staatsblatt* veröffentlicht worden ist ».

B.47.2. In den allgemeinen Erläuterungen zum Zusammenarbeitsabkommen vom 12. März 2012 heißt es:

« In Artikel 12 wird der zeitliche Geltungsbereich des Zusammenarbeitsabkommens festgelegt und seine Änderung oder Beendigung geregelt » (*Belgisches Staatsblatt* vom 12. April 2021, S. 32413; siehe auch *Parl. Dok.*, Kammer, 2020-2021, DOC 55-1853/001, S. 19).

B.48. In ihrem Gutachten zum Vorentwurf des Gesetzes, das zum angefochtenen Gesetz vom 2. April 2021 zur Billigung des Zusammenarbeitsabkommens vom 12. März 2021 geworden ist, hat die Gesetzgebungsabteilung des Staatsrates angemerkt:

« Conformément à l'article 12 de l'accord de coopération, celui-ci produit ses effets le 24 décembre 2020.

La non-rétroactivité des règles au niveau hiérarchique d'une norme législative est une garantie ayant pour but de prévenir l'insécurité juridique. Cette garantie exige que le contenu du droit soit prévisible et accessible, de sorte que le justiciable puisse prévoir, à un degré raisonnable, les conséquences d'un acte déterminé au moment où cet acte est accompli. La rétroactivité peut uniquement être justifiée lorsqu'elle est indispensable à la réalisation d'un objectif d'intérêt général.

En l'occurrence, la rétroactivité poursuit un objectif d'intérêt général, à savoir le maintien d'un cadre juridique offrant une sécurité juridique suffisante pour lutter contre la pandémie de COVID-19.

Ainsi qu'il a déjà été exposé dans les avis concernant les textes d'assentiment à l'accord de coopération relatif au traçage des contacts, un effet rétroactif peut, dans ces circonstances, être exceptionnellement conféré aux dispositions de l'accord de coopération qui correspondent sur le fond à ce qui a été réglé dans la réglementation fédérale, laquelle répond d'urgence à la nécessité de lutter contre la pandémie de COVID-19, à compter de la date d'entrée en vigueur de cette réglementation fédérale, plus particulièrement l'arrêté royal du 24 décembre 2020 ' concernant l'enregistrement et le traitement de données relatives aux vaccinations contre la COVID-19 '.

Cette justification ne vaut cependant pas pour les nouveaux éléments qui ne correspondent pas au traitement de données à caractère personnel tel qu'il s'est concrétisé dans les faits depuis cette date. Il faudra dès lors veiller à ce que les règles contenues dans cet accord de coopération s'accordent parfaitement avec cette concrétisation effective » (*Parl. Dok.*, Kammer, 2020-2021, DOC 55-1853/001, SS. 56-57; siehe auch *Parl. Dok.*, Flämisches Parlament, 2020-2021, Nr. 708/1, S. 92; *Parl. Dok.*, Wallonisches Parlament, 2020-2021, Nr. 509/1, SS. 86-87; *Parl. Dok.*, Parlament der Deutschsprachigen Gemeinschaft, 2020-2021, Nr. 132/1, SS. 34-35; *Parl. Dok.*, Vereinigte Versammlung der Gemeinsamen Gemeinschaftskommission, 2020-2021, Nr. B-65/1, SS. 20-21; *Parl. Dok.*, Versammlung der Französischen Gemeinschaftskommission, 2020-2021, Nr. 45/1, S. 35).

B.49.1. In dem Kontext, auf den in B.2 hingewiesen wurde, ist hervorzuheben, dass das Zusammenarbeitsabkommen vom 12. März 2021 innerhalb eines Zeitraums von weniger als

drei Monaten parallel zum Beginn der Impfkampagne im Januar 2021 unter den Umständen einer Notsituation abgeschlossen wurde, um die COVID-19-Pandemie zu bekämpfen.

Mit dem königlichen Erlass vom 24. Dezember 2020, der gemäß Artikel 11 des Gesetzes vom 22. Dezember 2020 ergangen ist, sowie mit dem Vereinbarungsprotokoll vom 27. Januar 2021 haben die verschiedenen Behörden des Landes die Rechtsgrundlage angenommen, die die Registrierung der Impfdaten bis zu einem Zusammenarbeitsabkommen ermöglichte.

B.49.2. Wie in B.4 erwähnt, übernimmt der Inhalt des Zusammenarbeitsabkommens den Inhalt des Vereinbarungsprotokolls vom 27. Januar 2021, das wiederum mit Anpassungen den Inhalt des königlichen Erlasses vom 24. Dezember 2020 übernommen hatte. Das Datum der Aufhebung des königlichen Erlasses vom 24. Dezember 2020 sowie das der Aufhebung des Vereinbarungsprotokolls vom 27. Januar 2021 sind das Datum, an dem das Zusammenarbeitsabkommen vom 12. März 2021 wirksam wird.

Aus dem Vorstehenden ergibt sich, dass die in Artikel 12 des Zusammenarbeitsabkommens vom 12. März 2021 enthaltene Rückwirkung durch das Ziel des Allgemeininteresses gerechtfertigt ist, die Rechtssicherheit durch die Konsolidierung und Ersetzung der Rechtsgrundlage für die Registrierung der Impfdaten in « Vaccinnet » sicherzustellen. Wie die Gesetzgebungsabteilung des Staatsrates betont hat, verfolgt diese Rückwirkung « ein Ziel des Allgemeininteresses, nämlich die Aufrechterhaltung eines rechtlichen Rahmens, der ausreichende Rechtssicherheit bietet, um die COVID-19-Pandemie zu bekämpfen » (*Parl. Dok.*, Kammer, 2020-2021, DOC 55-1853/001, S. 56).

B.49.3. Diese Rückwirkung hat außerdem keine unverhältnismäßigen Folgen. Dadurch, dass vorgesehen ist, dass das Zusammenarbeitsabkommen vom 12. März 2021 ab dem 24. Dezember 2020 wirksam ist, was die Bestimmungen betrifft, deren Inhalt dem Inhalt des königlichen Erlasses vom 24. Dezember 2020 « über die Registrierung und Verarbeitung von Daten über Impfungen gegen COVID-19 » entspricht, und ab dem 11. Februar 2021 wirksam ist, was die anderen Bestimmungen betrifft, beeinträchtigt Artikel 12 des Zusammenarbeitsabkommens vom 12. März 2021 nämlich die Rechtssicherheit und die berechtigten Erwartungen nicht, da er keinerlei Abänderung des Inhalts der zuvor bestehenden Regelung vornimmt, sondern sich darauf beschränkt, sie zu konsolidieren.

Es ist nämlich festzustellen, dass das Zusammenarbeitsabkommen für die Elemente, die der Verarbeitung personenbezogener Daten, wie sie durch den königlichen Erlass vom 24. Dezember 2020 vorgesehen war, entsprechen, zum Datum des Inkrafttretens dieses königlichen Erlasses wirksam wird, während das Zusammenarbeitsabkommen für die neuen Elemente, die nicht der Verarbeitung personenbezogener Daten, wie sie seit diesem Datum tatsächlich stattfand, entsprechen, zum Datum des Inkrafttretens des Vereinbarungsprotokolls vom 27. Januar 2021, das heißt dem 11. Januar 2021, wirksam wird. Diesbezüglich ist festzustellen, dass der in Artikel 4 § 2 Nr. 11 des Zusammenarbeitsabkommens vom 12. März 2021 erwähnte Zweck, den die klagende Partei beanstandet, bereits im Vereinbarungsprotokoll vom 27. Januar 2021 enthalten war.

B.50. Der dritte Teil des einzigen Klagegrunds, insofern er gegen die angefochtenen Akte gerichtet ist, insoweit damit Artikel 12 des Zusammenarbeitsabkommens vom 12. März 2021 gebilligt wird, ist unbegründet.

In Bezug auf den Antrag zur Aufrechterhaltung der Folgen

B.51. Die institutionellen Behörden beantragen die Aufrechterhaltung der Folgen der angefochtenen Akte im Fall einer Nichtigklärung.

B.52.1. Wenn eine gegen eine Gesetzesnorm gerichtete Nichtigkeitsklage begründet ist, hat der Gerichtshof gemäß Artikel 8 Absatz 1 des Sondergesetzes vom 6. Januar 1989 nur die Befugnis, den angefochtenen Akt vollständig oder teilweise für nichtig zu erklären.

Wenn er wie im vorliegenden Fall eine Gesetzesnorm für nichtig erklärt, kann der Gerichtshof gemäß Artikel 8 Absatz 3 des Sondergesetzes die Folgen einer für nichtig erklärten Bestimmung für die von ihm festgelegte Frist vorläufig aufrechterhalten, bis der Gesetzgeber der festgestellten Verfassungswidrigkeit ein Ende gesetzt hat.

B.52.2. 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*, ECLI:EU:C:2010:503). In Anbetracht dieser Rechtsprechung kann der Verfassungsgerichtshof folglich einem Antrag auf Aufrechterhaltung der Folgen eines für nichtig erklärten Gesetzgebungsaktes nicht stattgeben, da so die volle Wirksamkeit des Unionsrechts beeinträchtigt würde.

B.52.3. Im Übrigen ist in Anbetracht der begrenzten Tragweite der ausgesprochenen Nichtigerklärung diesem Antrag nicht stattzugeben.

Aus diesen Gründen:

Der Gerichtshof

- erklärt das Gesetz vom 2. April 2021, das Dekret der Flämischen Gemeinschaft vom 2. April 2021, das Dekret der Deutschsprachigen Gemeinschaft vom 29. März 2021, die Ordonnanz der Gemeinsamen Gemeinschaftskommission vom 2. April 2021, das Dekret der Wallonischen Region vom 1. April 2021 und das Dekret der Französischen Gemeinschaftskommission vom 1. April 2021 « zur Billigung des Zusammenarbeitsabkommens vom 12. März 2021 zwischen dem Föderalstaat, der Flämischen Gemeinschaft, der Französischen Gemeinschaft, der Deutschsprachigen Gemeinschaft, der Gemeinsamen Gemeinschaftskommission, der Wallonischen Region und der Französischen Gemeinschaftskommission über die Verarbeitung von Daten im Zusammenhang mit Impfungen gegen COVID-19 » für nichtig, insofern damit Artikel 5 des Zusammenarbeitsabkommens vom 12. März 2021 gebilligt wird, in dem Maße, in dem dieser Artikel die Übermittlung der in Artikel 3 § 2 des vorerwähnten Zusammenarbeitsabkommens erwähnten und in der Datenbank « Vaccinnet » gespeicherten Daten betrifft;

- weist die Klage im Übrigen zurück.

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 1. Juni 2023.

Der Kanzler,

Der Präsident,

F. Meersschaut

P. Nihoul