LOIS, DECRETS, ORDONNANCES ET REGLEMENTS
WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN

COUR CONSTITUTIONNELLE

[C − 2023/42867]

Extrait de l'arrêt n° 84/2023 du 1er juin 2023

Numéro du rôle : 7648

En cause : le recours en annulation de la loi du 2 avril 2021, du décret de la Communauté flamande du 2 avril 2021, du décret de la Communauté française du 25 mars 2021, du décret de la Communauté germanophone du 29 mars 2021, de l'ordonnance de la Commission communautaire commune du 2 avril 2021, du décret de la Région wallonne du 1er avril 2021 et du décret de la Commission communautaire française du 1er avril 2021 « portant assentiment à l'accord de coopération du 12 mars 2021 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 », introduit par Charlotte D'Hondt.

La Cour constitutionnelle,

composée des présidents P. Nihoul et L. Lavrysen, et des juges T. Giet, J. Moerman, M. Pâques, Y. Kherbache, T. Detienne, D. Pieters, S. de Bethune, E. Bribosia, W. Verrijdt et K. Jadin, assistée du greffier F. Meersschaut, présidée par le président P. Nihoul,

après en avoir délibéré, rend l'arrêt suivant :

I. *Objet du recours et procédure*

Par requête adressée à la Cour par lettre recommandée à la poste le 7 octobre 2021 et parvenue au greffe le 8 octobre 2021, Charlotte D'Hondt, assistée et représentée par Me P. Joassart, avocat au barreau de Bruxelles, a introduit un recours en annulation de la loi du 2 avril 2021, du décret de la Communauté flamande du 2 avril 2021, du décret de la Communauté française du 25 mars 2021, du décret de la Communauté germanophone du 29 mars 2021, de l'ordonnance de la Commission communautaire commune du 2 avril 2021, du décret de la Région wallonne du 1er avril 2021 et du décret de la Commission communautaire française du 1er avril 2021 « portant assentiment à l'accord de coopération du 12 mars 2021 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 » (publiés respectivement au *Moniteur belge* du 12 avril 2021, deuxième édition, du 9 avril 2021, du 6 avril 2021, du 12 avril 2021, deuxième édition, du 9 avril 2021, du 12 avril 2021, deuxième édition, et du 7 avril 2021).

(...)

II. *En droit*

(...)

Quant aux actes attaqués et à leur contexte

B.1. La partie requérante demande l'annulation de la loi du 2 avril 2021, du décret de la Communauté flamande du 2 avril 2021, du décret de la Communauté française du 25 mars 2021, du décret de la Communauté germanophone du 29 mars 2021, de l'ordonnance de la Commission communautaire commune du 2 avril 2021, du décret de la Région wallonne du 1er avril 2021 et du décret de la Commission communautaire française du 1er avril 2021 « portant assentiment à l'accord de coopération du 12 mars 2021 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 » (ci-après : l'accord de coopération du 12 mars 2021).

L'accord de coopération du 12 mars 2021 a été publié, dans les trois langues nationales, en annexe de la loi du 2 avril 2021, au *Moniteur belge* du 12 avril 2021.

B.2.1. Le 11 mars 2020, l'Organisation mondiale de la santé a qualifié de pandémie l'explosion du nombre de contaminations au coronavirus SARS-CoV-2. Depuis mars 2020, la Belgique aussi est confrontée à cette pandémie et à ses conséquences. Le coronavirus SARS-CoV-2 est un virus très contagieux, qui cause la COVID-19, maladie qui peut entraîner de sérieux problèmes médicaux, voire la mort, principalement chez les personnes âgées et chez les personnes ayant des comorbidités (*Doc. parl.*, Parlement flamand, 2019-2020, n° 415/1, p. 2; *Doc. parl.*, Parlement flamand, 2020-2021, n° 488/1, p. 2; *Doc. parl.*, Assemblée réunie de la Commission communautaire commune, 2019-2020, n° B-41/1, p. 1).

Dans le cadre de cette crise sanitaire et pour lutter contre la propagation de la COVID-19, le Conseil national de sécurité, d'abord, puis le Comité de concertation, qui regroupe des représentants de l'autorité fédérale et des entités fédérées, ont été chargés de prendre des mesures concertées afin de freiner cette propagation (*Doc. parl.*, Parlement flamand, 2019-2020, n° 415/1, p. 2; *Doc. parl.*, Parlement flamand, 2020-2021, n° 488/1, p. 2).

B.2.2. Les actes attaqués s'inscrivent dans le cadre visant à compléter et à actualiser l'arsenal des mesures que les différentes autorités ont prises pour lutter contre la pandémie de COVID-19 et contre la propagation du coronavirus SARS-CoV-2, ainsi qu'éviter une résurgence de la pandémie liée à la COVID-19. Les actes attaqués s'inscrivent plus précisément dans le cadre des mesures nécessaires pour l'organisation de la vaccination contre la COVID-19.

Comme dans d'autres pays participant à la procédure européenne d'achat des vaccins contre la COVID-19, dans laquelle la Commission européenne négocie avec les entreprises au nom des États membres, après autorisation de mise sur le marché et en fonction des capacités de production, l'autorité fédérale et les entités fédérées ont décidé de coopérer afin d'organiser une campagne de vaccination massive, volontaire et gratuite contre la COVID-19.

Cette décision s'est notamment fondée sur des études démontrant l'efficacité clinique de la vaccination à grande échelle contre le coronavirus très contagieux SARS-CoV-2 qui cause la maladie de la COVID-19, pour lutter contre la propagation des contaminations de cette maladie et éviter une surcharge des hôpitaux en raison des hospitalisations qui en découlent, ainsi que pour éviter une résurgence de la pandémie de COVID-19. L'Organisation mondiale de la santé conseille également au public de se faire vacciner contre la COVID-19.

La Conférence Interministérielle Santé publique du 16 novembre 2020 a défini les grands principes qui sous-tendent la stratégie belge de vaccination contre la COVID-19 :

- Objectif de couverture vaccinale de 70 % de la population;
- Détermination des groupes prioritaires sur la base d'avis scientifiques;

- Vaccination gratuite sur base volontaire pour chaque citoyen;

- Cofinancement de l'ensemble du programme de vaccination par l'autorité fédérale et les entités fédérées.

Ces décisions dépendent des éléments suivants :

- Des campagnes de vaccination de masse, les vaccins étant fournis dans des flacons multidoses qui doivent être administrés le même jour;

- La mise à la disposition de la Belgique d'un ou de plusieurs vaccins efficaces et sûrs contre la COVID-19.

- La capacité du système de santé belge à distribuer et à vacciner progressivement et efficacement la population, les autorités de santé étant soutenues par la Task force interfédérale « vaccin COVID-19 » créée par la Conférence Interministérielle Santé publique le 16 novembre 2020, l'ensemble des structures de santé du pays dont Sciensano et l'Agence fédérale des médicaments et des produits de santé (AFMPS). Le logiciel d'enregistrement Vaccinnet+ sera utilisé par toutes les entités fédérées à cette fin;

- La volonté de surmonter, par la persuasion et la transparence, l'hésitation vaccinale et d'obtenir ainsi l'adhésion de la population à cette stratégie de santé publique.

La stratégie de vaccination contre la COVID-19 s'est déployée en plusieurs phases, dès le mois de janvier 2021, avec une hiérarchisation des groupes cibles, les groupes prioritaires étant les résidents de maisons de repos et une partie des membres du personnel des maisons de repos, le personnel hospitalier et le personnel de soins et d'aide œuvrant en première ligne. Dès février 2021, les groupes prioritaires ont été étendus aux personnes à risques présentant des comorbidités, aux personnes âgées de 65 ans et plus et aux personnes âgées de 18 à 55 ans dans les forces de police, avant d'être progressivement élargis, sur la base du critère de l'âge et de la vulnérabilité, à toute la population de plus de 18 ans, puis de plus de 16 ans, plus de 12 ans et, enfin, à partir de 5 ans.

Sur la base des connaissances scientifiques actualisées, un schéma vaccinal d'une ou de deux doses de vaccin, en fonction du vaccin administré, a été établi par la Task force interfédérale « vaccin COVID-19 », et la possibilité de bénéficier d'une dose « booster » a également été offerte à la population.

B.2.3.1. Cette campagne de vaccination massive est également étroitement liée aux nouvelles mesures prises en juillet 2020 afin de lutter contre les risques de propagation liés aux assouplissements des restrictions des contacts physiques et à la possibilité de voyager à nouveau, compte tenu de la nouvelle phase de la crise de la COVID-19.

B.2.3.2. Le règlement (UE) 2021/953 du Parlement européen et du Conseil du 14 juin 2021 « relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de COVID-19 » (ci-après : le règlement (UE) 2021/953) prévoit, aux termes de son article 1er, paragraphe 1, un cadre pour la délivrance, la vérification et l'acceptation du certificat COVID numérique de l'UE, à savoir un certificat interopérable contenant des informations sur la vaccination, les résultats des tests ou le rétablissement de son titulaire, délivré dans le contexte de la pandémie de COVID-19, et ce afin de faciliter l'exercice, par les titulaires de tels certificats, du droit à la libre circulation pendant la pandémie de COVID-19.

Le certificat COVID numérique de l'UE permet la délivrance, la vérification et l'acceptation transfrontières, notamment, d'un certificat de vaccination confirmant que le titulaire a reçu un vaccin contre la COVID-19 dans l'État membre qui délivre le certificat.

Les considérants 8 et 29 du règlement (UE) 2021/953 indiquent :

« 8. De nombreux États membres ont lancé ou prévoient de lancer des initiatives visant à délivrer des certificats de vaccination COVID-19. Toutefois, pour que ces certificats de vaccination puissent être utilisés de manière efficace dans un contexte transfrontière lorsque les citoyens de l'Union exercent leur droit à la libre circulation, ils doivent être pleinement interopérables, compatibles, sûrs et vérifiables. Une approche commune entre les États membres est nécessaire pour ce qui est du contenu, du format, des principes, des normes techniques et du niveau de sécurité de ces certificats de vaccination.

[...]

29. Dans l'optique de faciliter la libre circulation et pour garantir que les restrictions à la libre circulation actuellement en place pendant la pandémie de COVID-19 peuvent être levées de manière coordonnée sur la base des preuves scientifiques les plus récentes et des orientations mises à disposition par le comité de sécurité sanitaire institué par l'article 17 de la décision n° 1082/2013/UE du Parlement européen et du Conseil, l'ECDC et l'Agence européenne des médicaments (EMA), il convient de mettre en place un certificat de vaccination interopérable. Un tel certificat de vaccination devrait servir à confirmer que son titulaire a été vacciné contre la COVID-19 dans un État membre et devrait contribuer à la levée progressive des restrictions à la libre circulation. Le certificat de vaccination ne devrait contenir que les informations nécessaires pour identifier clairement le titulaire ainsi que le vaccin contre la COVID-19 qui a été administré, le nombre de doses ainsi que la date et le lieu de vaccination. Les États membres devraient délivrer des certificats de vaccination aux personnes ayant reçu des vaccins contre la COVID-19 pour lesquels une autorisation de mise sur le marché a été délivrée en vertu du règlement (CE) n° 726/2004 du Parlement européen et du Conseil, aux personnes ayant reçu des vaccins contre la COVID-19 pour lesquels une autorisation de mise sur le marché a été délivrée par l'autorité compétente d'un État membre en vertu de la directive 2001/83/CE du Parlement et du Conseil, et aux personnes ayant reçu des vaccins contre la COVID-19 dont la distribution a été temporairement autorisée en vertu de l'article 5, paragraphe 2, de ladite directive ».

Intitulé « Certificat de vaccination », l'article 5 du règlement (UE) 2021/953 dispose :

« 1. Chaque État membre délivre, automatiquement ou à la demande des personnes concernées, les certificats de vaccination visés à l'article 3, paragraphe 1, point a), aux personnes à qui un vaccin contre la COVID-19 a été administré. Ces personnes sont informées de leur droit à un certificat de vaccination.

2. Le certificat de vaccination contient les catégories suivantes de données à caractère personnel :

"a") l'identité du titulaire;

"b") des informations sur le vaccin contre la COVID-19 administré et sur le nombre de doses administrées au titulaire;

"c") les métadonnées du certificat, telles que l'émetteur du certificat ou un identifiant unique du certificat.

Les données à caractère personnel sont incluses dans le certificat de vaccination conformément aux champs de données spécifiques indiqués au point 1 de l'annexe.

La Commission est habilitée à adopter des actes délégués conformément à l'article 12 pour modifier le point 1 de l'annexe en modifiant ou en supprimant des champs de données, ou en ajoutant des champs de données relevant des catégories de données à caractère personnel visées aux points b) et c) du premier alinéa du présent paragraphe, lorsqu'une telle modification est nécessaire pour vérifier et confirmer l'authenticité, la validité et l'intégrité du certificat de vaccination, en cas de progrès scientifiques accomplis dans la maîtrise de la pandémie de COVID-19, ou pour assurer l'interopérabilité avec les normes internationales.

3. Le certificat de vaccination est délivré dans un format sécurisé et interopérable conformément à l'article 3, paragraphe 2, après l'administration de chaque dose et indique clairement si le schéma de vaccination est achevé ou non.

4. Lorsque, en cas d'émergence de nouvelles preuves scientifiques ou pour assurer l'interopérabilité avec les normes internationales et les systèmes technologiques, des raisons d'urgence impérieuses l'imposent, la procédure prévue à l'article 13 est applicable aux actes délégués adoptés en vertu du présent article.

5. Si les États membres acceptent une preuve de vaccination afin de lever les restrictions à la libre circulation mises en place, conformément au droit de l'Union, pour limiter la propagation du SARS-CoV-2, ils acceptent également, dans les mêmes conditions, les certificats de vaccination délivrés par d'autres États membres conformément au présent règlement pour un vaccin contre la COVID-19 pour lequel une autorisation de mise sur le marché a été délivrée en vertu du règlement (CE) nº 726/2004.

Les États membres peuvent également accepter, aux mêmes fins, des certificats de vaccination délivrés par d'autres États membres conformément au présent règlement pour un vaccin contre la COVID-19 pour lequel une autorisation de mise sur le marché a été délivrée par l'autorité compétente d'un État membre en vertu de la directive 2001/83/CE, un vaccin contre la COVID-19 dont la distribution a été autorisée temporairement en vertu de l'article 5, paragraphe 2, de ladite directive, ou un vaccin contre la COVID-19 pour lequel la procédure d'inscription sur la liste d'utilisation d'urgence de l'OMS est terminée.

Si les États membres acceptent des certificats de vaccination pour un vaccin contre la COVID-19 visé au deuxième alinéa, ils acceptent également, dans les mêmes conditions, les certificats de vaccination délivrés par d'autres États membres conformément au présent règlement pour le même vaccin contre la COVID-19 ».

L'annexe intitulée « Ensemble des données des certificats » prévoit en son point 1 :

« Champs de données à inclure dans le certificat de vaccination :

a) nom : nom(s) de famille et prénom(s), dans cet ordre;

b) date de naissance;

c) maladie ou agent ciblé : COVID-19 (SARS-CoV-2 ou l'un de ses variants);

d) vaccin ou prophylaxie contre la COVID-19;

e) dénomination du vaccin contre la COVID-19;

f) titulaire de l'autorisation de mise sur le marché ou fabricant du vaccin contre la COVID-19;

g) nombre dans une série de doses ainsi que le nombre total de doses dans la série;

h) date de la vaccination, indiquant la date de la dernière dose reçue;

i) État membre ou pays tiers dans lequel le vaccin a été administré;

j) émetteur du certificat;

k) identifiant unique du certificat ».

B.2.3.3. L'exposé général de l'accord de coopération du 11 juin 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant l'opérationnalisation du Règlement (UE) du Parlement Européen et du Conseil relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats interopérables de vaccination, de test et de rétablissement afin de faciliter la libre circulation pendant la pandémie de COVID-19 (Certificat Numérique COVID de l'UE) indique :

« L'accord de coopération du 12 mars 2021 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 [...] régit le système d'information commun qui est mis en place pour l'invitation à la vaccination des personnes, pour l'organisation de la vaccination et pour l'enregistrement de la vaccination. Les entités fédérées et l'autorité fédérale considèrent la mise en place d'un système d'information commun comme une condition fondamentale. En vue de soutenir l'invitation des personnes à se faire vacciner et l'organisation de la vaccination, un système d'information commun était nécessaire afin d'éviter que les personnes ne soient invitées de manière non coordonnée ou que des personnes déjà vaccinées soient à nouveau invitées. Par ailleurs, le système doit permettre d'identifier le schéma posologique adéquat, notamment en ce qui concerne les différentes doses d'un vaccin à administrer (intervalle optimal proposé en cas de vaccins multidoses) et doit veiller à ce que l'organisation de la vaccination se déroule de manière optimale en fonction de la disponibilité du matériel et du personnel (médical) nécessaires. L'enregistrement des vaccinations dans un système d'information commun (Vaccinnet) par les vaccinateurs flamands, wallons, bruxellois et germanophones était notamment nécessaire. Compte tenu du fait qu'il s'agit d'une nécessité et qu'elle concerne le traitement de données à caractère personnel, une telle obligation d'enregistrement requiert une base juridique solide. La base de données est créée et gérée en collaboration très étroite entre les entités fédérées et l'Etat fédéral. Il est donc également approprié d'utiliser le même système opérationnel pour la délivrance des certificats » (*Moniteur belge* du 14 juin 2021, deuxième édition, p. 61955).

B.2.3.4. Les accords de coopération du 14 juillet 2021 et du 27 septembre 2021 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 des données liées au certificat COVID numérique de l'UE et au COVID Safe Ticket, le PLF et le traitement des données à caractère personnel des travailleurs salariés et des travailleurs indépendants vivant ou résidant à l'étranger qui effectuent des activités en Belgique , ainsi que l'accord de coopération du 28 octobre 2021 modifiant celui du 14 juillet 2021 définissent une base juridique pour l'utilisation nationale du certificat COVID numérique de l'UE et la génération du COVID Safe Ticket (ci-après : le CST) basée sur le certificat COVID numérique de l'UE. La vaccination d'une personne contre la COVID-19 permet de générer automatiquement le CST.

L'exposé général de l'accord de coopération du 14 juillet 2021, précité, indique à cet égard que, selon les connaissances scientifiques disponibles au moment de l'adoption de l'accord, les personnes qui ont été vaccinées présentent un risque moindre de contaminer d'autres personnes avec le coronavirus SARS-CoV-2 (*Moniteur belge* du 23 juillet 2021, p. 76172; voy. aussi le considérant 7 du règlement (UE) 2021/953).

L'article 11 de l'accord de coopération du 14 juillet 2021 dispose :

« § 1er. Aux fins de la vérification et pour la création et la délivrance du certificat COVID numérique de l'UE aux titulaires d'un certificat de vaccination, certificat de test ou certificat de rétablissement, les catégories de données à caractère personnel suivantes sont traitées conformément au règlement relatif au certificat COVID numérique de l'UE :

1° les catégories de données à caractère personnel visées à l'article 9, §§ 1, 2 ou 3;

2° le numéro d'identification visé à l'article 8 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale; et

3° la résidence principale, visées à l'article 3, premier alinéa, 5°, de la loi du 8 août 1983 organisant un registre national des personnes physique;

§ 2. Les catégories de données à caractère personnel mentionnées au § 1 sont obtenues à partir des banques de données suivantes :

[...]

2° Vaccinnet : en ce qui concerne le numéro d'identification visé à l'article 8 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale et les catégories de données à caractère personnel dans le certificat de vaccination, décrites à l'article 9, § 1;

[...]

§ 4. Par dérogation à l'article 3, § 1, de l'accord de coopération du 25 août 2020 et à l'article 4, § 2, de l'accord de coopération du 12 mars 2021, les données à caractère personnel visées au § 1, peuvent être traitées pour les finalités de traitement visées à l'article 10 par les responsables du traitement, pour l'exercice de leurs missions légales définies dans le présent accord de coopération, les entités fédérées et Sciensano ».

B.3.1. Par l'accord de coopération du 12 mars 2021, l'autorité fédérale et les entités fédérées ont mis en place « le système d'information commun [...] pour l'invitation à la vaccination des personnes, pour l'organisation de la vaccination et pour l'enregistrement de la vaccination » (*Moniteur belge* du 12 avril 2021, deuxième édition, p. 32397) :

« L'enregistrement des vaccinations dans un système d'information commun (Vaccinnet) par les vaccinateurs flamands, wallons, bruxellois et germanophones est notamment nécessaire pour mener une gestion de crise optimale, permettre la pharmacovigilance, comme visée à l'article 4, 2°, du présent accord, suivre le taux de vaccination de la population et estimer l'impact sur l'assurance maladie.

Compte tenu du fait qu'il s'agit d'une nécessité et qu'elle concerne le traitement de données à caractère personnel, une telle obligation d'enregistrement requiert une base juridique solide.

La base de données est créée et gérée en collaboration très étroite entre les entités fédérées et l'Etat fédéral » (*ibid.*, pp. 32397-32398).

B.3.2. Dans ce contexte, l'accord de coopération du 12 mars 2021 organise deux bases de données différentes.

D'une part, une première base de données contenant les codes de vaccination est créée « afin d'assurer, la campagne de vaccination massive dans le contexte de la pandémie de COVID-19 en permettant l'invitation des personnes à se faire vacciner, l'identification du schéma posologique adéquat et de la bonne organisation de la vaccination en fonction de la disponibilité des vaccins et du matériel ainsi que du personnel (médical et infirmier) nécessaires à cet effet » (*ibid.*, p. 32398).

Cette banque de données génère un code de vaccination aléatoire pour l'ensemble de la population *a priori* vaccinable, et recueille les données relatives à ces personnes afin de coordonner le schéma de vaccination contre la COVID-19 et éviter de générer un nouveau code de vaccination pour une personne qui a déjà été vaccinée (article 2, § 1er). Les données enregistrées dans cette banque de données sont identifiées par l'article 3, § 1er, de l'accord de coopération du 12 mars 2021. Elles sont conservées jusqu'à cinq jours à compter du lendemain de la publication de l'arrêté royal annonçant la fin de l'épidémie due au coronavirus SARS-CoV-2 (article 6, § 1er).

D'autre part, une seconde base de données, « Vaccinnet », concerne l'enregistrement pour l'ensemble du pays, par la personne qui a administré le vaccin contre la COVID-19 ou son mandataire, des données de vaccination, en tant que telles, des personnes qui se sont fait vacciner (article 2, § 2). Les données de vaccination sont définies par l'article 3, § 2, de l'accord de coopération du 12 mars 2021 comme étant les données d'identité de la personne à laquelle le vaccin a été administré (1°), les données d'identité et de contact éventuelles de la personne qui a administré le vaccin (2°), les données relatives au vaccin (3°), la date et le lieu d'administration de chaque dose du vaccin (4°), les données relatives au schéma de vaccinations contre la COVID-19 de la personne à laquelle est administré le vaccin (5°) et, le cas échéant, les données relatives aux effets indésirables observés pendant ou après la vaccination sur la personne concernée, dont la personne qui a administré le vaccin ou son mandataire a connaissance (6°). Ces données sont conservées jusqu'au décès de la personne à laquelle le vaccin contre la COVD-19 a été administré et pendant 30 ans au minimum à compter de la vaccination (article 6, § 2).

La banque de données « Vaccinnet » « vise plusieurs objectifs en lien avec la vaccination : il s'agit de la prestation de soins de santé de qualité, la pharmacovigilance, la traçabilité des vaccins, la gestion de schémas de vaccination, l'organisation logistique de la vaccination, la détermination du taux de vaccination, l'organisation du suivi des contacts, l'exécution du suivi et de la surveillance, le calcul de la répartition des coûts de vaccination, l'exécution d'études scientifiques ou statistiques » (*ibid.*, p. 32400).

Les finalités de traitement des données enregistrées dans les deux banques de données sont mentionnées dans l'article 4 de l'accord de coopération du 12 mars 2021. Les données recueillies dans ces deux banques de données « ne peuvent pas être transmises à des tiers sauf lorsqu'une loi, un décret ou une ordonnance autorisent un tiers à avoir accès ou à recevoir de telles données et ce, uniquement pour qu'ils puissent poursuivre les mêmes finalités liées à la vaccination que celles visées à l'article 4 de l'accord de coopération » (*ibid.*, p. 32401), après autorisation par le Comité de sécurité de l'information.

Pour les deux banques de données, les entités fédérées compétentes ou les agences désignées par les entités fédérées compétentes et l'autorité fédérale agissent, chacune dans le cadre de leur compétence, en tant que responsables du traitement des données (article 7, § 1er). Pour les personnes qui ressortissent aux compétences de l'Autorité fédérale, Sciensano est identifié comme le responsable du traitement des données (article 7, § 1er, 7°). Un point de contact centralisé par entité et un droit d'accès électronique sont prévus (article 7, § 2).

La mise en œuvre et le respect de l'accord de coopération du 12 mars 2021 sont surveillés par la Conférence interministérielle Santé publique (article 9, § 1er).

B.4.1. Les dispositions de l'accord de coopération du 12 mars 2021 correspondent en substance à celles de l'arrêté royal du 24 décembre 2020 « concernant l'enregistrement et le traitement de données relatives aux vaccinations contre la COVID-19 » (ci-après : l'arrêté royal du 24 décembre 2020), contre lequel la partie requérante a également introduit un recours en annulation devant le Conseil d'État. Le préambule de cet arrêté royal indiquait qu'« il est d'une importance vitale pour la santé publique et pour éviter une résurgence de la pandémie liée au COVID-19, que les mesures nécessaires en matière de vaccinations puissent être prises » (*Moniteur belge* du 24 décembre 2020, deuxième édition, p. 94404), dans l'attente de la conclusion d'un accord de coopération.

Cet arrêté royal est entré en vigueur le 24 décembre 2020, date de sa publication au *Moniteur belge*.

L'article 9 de l'arrêté royal du 24 décembre 2020 disposait :

« 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. L'arrêté royal du 24 décembre 2020 a été pris conformément à l'article 11 de la loi du 22 décembre 2020 « portant diverses mesures relatives aux tests antigéniques rapides et concernant l'enregistrement et le traitement de données relatives aux vaccinations dans le cadre de la lutte contre la pandémie de COVID-19 » (ci-après : la loi du 22 décembre 2020), qui disposait :

« Le médecin ou l'infirmier qui administre un vaccin contre la COVID-19 ou qui supervise la vaccination enregistre chaque vaccination dans la base de données désignée par la Conférence interministérielle Santé publique. Le Roi précise, par arrêté délibéré en Conseil des ministres, les modalités de cet enregistrement et définit au moins les finalités du traitement de données, les catégories de personnes à propos desquelles des données sont traitées, les catégories de données traitées, les responsables du traitement des données ainsi que la durée de conservation des données ».

B.4.2.2. Les travaux préparatoires de la loi du 22 décembre 2020 exposent à cet égard :

« 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 » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1677/001, pp. 10-11).

B.4.2.3. L'article 11 de la loi du 22 décembre 2020 a été abrogé par l'article 11 de l'accord de coopération du 12 mars 2021.

B.4.3. Le préambule de l'arrêté royal du 24 décembre 2020 indique que la base de données des vaccinations a été désignée par la Conférence interministérielle Santé publique du 3 décembre 2020 (*Moniteur belge* du 24 décembre 2020, p. 94404). L'article 1er, 2°, de l'arrêté royal du 24 décembre 2020 définit la « base de données des vaccinations » comme « la base de données désignée par la Conférence interministérielle Santé publique en vertu de l'article 11 de la loi du 22 décembre 2020 portant diverses mesures relatives aux tests antigéniques rapides et concernant l'enregistrement et le traitement de données relatives aux vaccinations dans le cadre de la lutte contre la pandémie de COVID-19 ».

Au sujet de cette banque de données, les travaux préparatoires de la loi du 22 décembre 2020 indiquent :

« 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 » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1677/002, p. 4).

B.4.4.1. Un protocole d'accord du 27 janvier 2021 « 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 » (ci-après : le protocole d'accord du 27 janvier 2021) reprend en grande partie le contenu des dispositions de l'arrêté royal du 24 décembre 2020. Le préambule de ce protocole d'accord indique que ce protocole « a pu être réalisé en respect de la répartition de compétences qui en vertu de la loi spéciale de réformes institutionnelles ont été attribuées aux différents niveaux de pouvoirs grâce à une collaboration intense au sein de la Conférence Interministérielle qui s'inscrit dans une longue tradition de collaboration au sein de la Conférence Interministérielle de santé entre les différents niveaux de pouvoirs de notre pays » et que, « dans le cadre de la vaccination contre la COVID-19, un enregistrement des données de vaccination dans une base de données commune par les vaccinateurs flamands, bruxellois, wallons et germanophones est absolument nécessaire pour diverses finalités » (*Moniteur belge* du 11 février 2021, p. 13033).

L'article 1er, 3°, du protocole d'accord du 27 janvier 2021 définit « Vaccinnet » comme « le système d'enregistrement visé à l'article 9 de l'arrêté du Gouvernement flamand du 16 mai 2014 portant diverses dispositions en exécution du décret [flamand] du 21 novembre 2003 relatif à la politique de santé préventive et modifiant des arrêtés d'exécution de ce décret ». Conformément à l'article 43 du décret, précité, du 21 novembre 2003, les vaccinateurs doivent collaborer au système d'enregistrement « Vaccinnet » lorsque, sur la base de sa compétence en matière de politique de santé préventive, le Gouvernement flamand établit un schéma de vaccination qui reprend les vaccinations recommandées pour la population.

La banque de données « Vaccinnet » visée dans le protocole d'accord du 27 janvier 2021 constitue ainsi une extension, concernant les vaccinations contre la COVID-19, de la banque de données existante « Vaccinnet », créée au niveau de la Communauté flamande. La répartition du coût de développement de « Vaccinnet » a été fixée dans l'article 6 du protocole d'accord du 9 février 2022 conclu entre le Gouvernement fédéral et les autorités visées aux articles 128, 130 et 135 de la Constitution « concernant le cofinancement du programme de vaccination contre la COVID-19 ».

B.4.4.2. L'article 11 du protocole d'accord du 27 janvier 2021 dispose :

« Le présent protocole d'accord n'est pas un accord de coopération au sens de l'article 92*bis* 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 ».

L'article 12 du protocole d'accord du 27 janvier 2021 dispose :

« 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. Conformément à son article 12, alinéa 1er, l'accord de coopération du 12 mars 2021 produit ses effets à partir du 24 décembre 2020 pour ce qui concerne les dispositions dont le contenu correspond à celui de l'arrêté royal du 24 décembre 2020 concernant l'enregistrement et le traitement de données relatives aux vaccinations contre la COVID-19 et à partir du 11 février 2021 pour ce qui concerne les autres dispositions.

Conformément à l'article 9 de l'arrêté royal du 24 décembre 2020 et à l'article 12 du protocole d'accord du 27 janvier 2021, l'arrêté royal du 24 décembre 2020 et le protocole d'accord du 27 janvier 2021 ont cessé de produire leurs effets le jour de l'entrée en vigueur de l'accord de coopération du 12 mars 2021, soit le 22 avril 2021.

B.6. Les sept législations attaquées (ci-après : les actes attaqués) se limitent à porter assentiment à l'accord de coopération du 12 mars 2021.

Quant à la recevabilité ratione temporis *du recours*

B.7. Le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté française, le Gouvernement de la Communauté germanophone, le Collège de la Commission communautaire française et le Collège réuni de la Commission communautaire commune estiment que le recours en annulation, introduit le 7 octobre 2021, est manifestement irrecevable *ratione temporis* en ce qu'il est dirigé contre le décret d'assentiment de la Communauté française du 25 mars 2021, publié au *Moniteur belge* le 6 avril 2021.

B.8.1. Pour satisfaire aux exigences de l'article 3, § 1er, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, un recours en annulation doit être introduit dans le délai de six mois suivant la publication de la norme attaquée au *Moniteur belge*.

B.8.2. La disposition précitée n'établit aucune distinction quant à la prise d'effet du délai de recours en annulation dirigé contre la norme attaquée, selon qu'elle porte ou non assentiment à un accord de coopération.

Contrairement à ce qu'allègue la partie requérante, le délai pour introduire un recours en annulation contre des actes d'assentiment à un accord de coopération ne prend pas cours à dater de l'entrée en vigueur de cet accord de coopération, mais commence à courir à la date de la publication des actes attaqués.

B.8.3. Dans une série d'arrêts précédents, la Cour a déjà indiqué que, pour fixer le délai d'introduction d'un recours ou d'une demande de suspension, il faut – à défaut de précision dans la loi spéciale du 6 janvier 1989 et par analogie avec le régime de l'article 54 du Code judiciaire – calculer de quantième à veille de quantième (voy. l'arrêt n° 125/2012 du 18 octobre 2012, ECLI:BE:GHCC:2012:ARR.125, B.2; l'arrêt n° 169/2016 du 22 décembre 2016, ECLI:BE:GHCC:2016:ARR.169, B.2).

Le décret d'assentiment de la Communauté française du 25 mars 2021 a été publié au *Moniteur belge* du 6 avril 2021. Le délai pour introduire un recours contre cet acte a donc pris cours le 7 avril 2021 et a expiré le 6 octobre 2021. Il s'ensuit que le recours en annulation introduit par requête déposée à la poste le 7 octobre 2021 est manifestement irrecevable.

B.8.4. En ce qu'il est dirigé contre le décret d'assentiment de la Communauté française du 25 mars 2021, le recours en annulation est irrecevable *ratione temporis*.

Quant à l'étendue du recours en annulation

B.9.1. Pour satisfaire aux exigences de l'article 6 de la loi spéciale du 6 janvier 1989, les moyens de la requête doivent faire connaître, parmi les règles dont la Cour garantit le respect, celles qui seraient violées ainsi que les dispositions qui violeraient ces règles et exposer en quoi ces règles auraient été transgressées par ces dispositions.

B.9.2. La Cour détermine l'étendue du recours en annulation en fonction du contenu de la requête et en particulier sur la base de l'exposé des moyens. La Cour limite son examen aux dispositions contre lesquelles des griefs sont effectivement dirigés.

B.10.1. Il ressort de l'exposé du moyen unique que les griefs de la partie requérante ne sont dirigés contre les actes attaqués qu'en ce qu'ils portent assentiment à certaines dispositions de l'accord de coopération du 12 mars 2021 qui organisent l'enregistrement et le traitement des données à caractère personnel dans la banque de données « Vaccinnet », que la partie requérante identifie expressément dans son moyen :

- l'article 2, § 2, qui vise l'enregistrement des données de vaccination;
- l'article 3, § 2, qui détermine les données de vaccination recueillies dans « Vaccinnet »;
- l'article 4, § 2, qui fixe les finalités pour le traitement des données visées à l'article 3, § 2;
- l'article 5, qui permet la communication à des tiers des données figurant dans « Vaccinnet »;
- l'article 6, § 2, qui fixe la durée de conservation des données visées à l'article 3, § 2;
- l'article 12, qui fixe la date d'entrée en vigueur des dispositions de l'accord de coopération du 12 mars 2021.

B.10.2. Cependant, lorsqu'elle critique ces dispositions dans son moyen unique, la partie requérante ne formule aucun grief contre le principe même de l'enregistrement des données de vaccination, ni contre les données de vaccination recueillies dans « Vaccinnet ». En dehors d'une critique générale, elle n'expose pas en quoi, en portant assentiment aux articles 2, § 2, et 3, § 2, de l'accord de coopération du 12 mars 2021, les actes attaqués violeraient les dispositions visées dans le moyen.

En ce qu'il vise ces dispositions, le moyen unique ne répond dès lors pas aux exigences de l'article 6 de la loi spéciale du 6 janvier 1989.

B.10.3. La Cour limite par conséquent son examen du recours en annulation dirigé contre les actes attaqués en ce qu'ils portent assentiment aux articles 4, § 2, 5 et 6, § 2, de l'accord de coopération du 12 mars 2021, et à l'article 12 de l'accord de coopération, précité, en ce que ce dernier fixe la date d'entrée en vigueur des articles 4, § 2, 5 et 6, § 2, précités.

Le recours en annulation est par conséquent irrecevable en ce qu'il est dirigé contre les actes attaqués en ce qu'ils portent assentiment aux autres dispositions de l'accord de coopération précité.

B.10.4. La Cour rappelle qu'elle ne peut utilement contrôler les actes attaqués sans impliquer dans son examen le contenu des dispositions pertinentes de l'accord de coopération précité.

Quant à l'intérêt de la partie requérante

B.11. La partie requérante justifie son intérêt à agir par le fait qu'elle est une personne physique résidant en Belgique et qu'elle est susceptible de se faire vacciner contre la COVID-19, de sorte que les actes attaqués peuvent l'affecter directement et défavorablement. En effet, si elle décide de se faire vacciner, son nom et ses différentes données à caractère personnel figureront dans « Vaccinnet », en violation de son droit au respect de la vie privée, lu en combinaison avec le principe de la non-rétroactivité des lois. Si, par contre, elle décide de ne pas se faire vacciner, il existerait un risque sérieux que des restrictions l'affectent en raison de sa non-vaccination.

B.12. Le Conseil des ministres, le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté française, le Gouvernement de la Communauté germanophone, le Collège de la Commission communautaire française et le Collège réuni de la Commission communautaire commune contestent l'intérêt à agir de la partie requérante, estimant que son action s'apparente à un recours populaire.

B.13. La Constitution et la loi spéciale du 6 janvier 1989 imposent à toute personne physique ou morale qui introduit un recours en annulation de justifier d'un intérêt. Ne justifient de l'intérêt requis que les personnes dont la situation pourrait être affectée directement et défavorablement par la norme attaquée.

B.14.1. En vertu de l'article 2, § 1er, non attaqué, de l'accord de coopération du 12 mars 2021, toute personne physique se trouvant sur le territoire de la Belgique est appelée à recevoir une invitation à se faire vacciner par le biais d'un code de vaccination contre la COVID-19, conformément à la stratégie de vaccination définie par les autorités compétentes. Ce code de vaccination sans signification est généré par la banque de données organisée conformément à l'article 3, § 1er, non attaqué, de l'accord de coopération du 12 mars 2021.

Conformément à l'article 2, § 2, de l'accord de coopération du 12 mars 2021, chaque vaccination donne lieu à l'enregistrement, dans « Vaccinnet », des données de vaccination mentionnées à l'article 3, § 2, de l'accord de coopération du 12 mars 2021. Toutes les personnes qui se font vacciner contre la COVID-19 sont par conséquent soumises à l'enregistrement automatique de leurs données de vaccination dans la banque de données « Vaccinnet » et aux traitements de ces données conformément à ce que prévoit cet accord de coopération.

En sa qualité de personne physique se trouvant sur le territoire de la Belgique, la partie requérante a nécessairement été invitée à se faire vacciner et elle ne pouvait accepter l'invitation de se faire vacciner qu'en donnant son consentement pour que ses données de vaccination soient enregistrées et traitées dans « Vaccinnet » conformément aux actes attaqués portant assentiment à l'accord de coopération du 12 mars 2021. Les implications des actes attaqués en matière de traitement des données de vaccination sont dès lors susceptibles d'influencer directement le choix de la partie requérante quant à sa vaccination contre la COVID-19.

B.14.2. Il découle de ce qui précède que les actes attaqués sont susceptibles d'affecter directement et défavorablement la partie requérante dans sa décision de se faire vacciner.

B.14.3. Pour le surplus, l'accord de coopération du 12 mars 2021 se limite à organiser le système commun pour l'enregistrement des données de vaccination contre la COVID-19 sur le territoire de la Belgique. Cet accord de coopération ne crée aucune obligation vaccinale, la stratégie vaccinale exposée en B.2.2 étant fondée sur une vaccination volontaire et gratuite.

Contrairement à ce qu'allègue la partie requérante, les actes attaqués ne prévoient aucune conséquence qui serait liée à l'absence de vaccination. Les incidences d'un certificat de vaccination, mais également d'un certificat de test et de rétablissement, pour l'obtention d'un CST, sont quant à elles déterminées dans les accords de coopération du 14 juillet 2021, du 27 septembre 2021 et du 28 octobre 2021, cités en B.2.3.4. Non seulement la partie requérante ne démontre pas la réalité des restrictions qu'elle invoque et qui découleraient de l'absence de vaccination – ce qui suffit pour établir que le préjudice allégué est purement hypothétique –, mais ces éventuelles restrictions ne constituent pas un préjudice qui découlerait directement des actes attaqués par le recours présentement examiné.

En ce qu'elle invoque les conséquences liées à la non-vaccination contre la COVID-19, la partie requérante ne justifie pas de l'intérêt requis.

Quant au fond

B.15. Le moyen unique est pris de la violation de l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, avec les articles 5, 6, 9 et 35 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) » (ci-après : le RGPD), ainsi qu'avec le principe de la non-rétroactivité des lois.

B.16.1. L'article 22 de la Constitution dispose :

« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.

La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ».

B.16.2. L'article 8 de la Convention européenne des droits de l'homme dispose :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

B.16.3. Le Constituant a recherché la plus grande concordance possible entre l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme (*Doc. parl.*, Chambre, 1992-1993, n° 997/5, p. 2).

La portée de cet article 8 est analogue à celle de la disposition constitutionnelle précitée, de sorte que les garanties que fournissent ces deux dispositions forment un tout indissociable.

B.16.4. Le droit au respect de la vie privée, tel qu'il est garanti par les dispositions constitutionnelles et conventionnelles précitées a pour but essentiel de protéger les personnes contre les ingérences dans leur vie privée.

Ce droit a une portée étendue et englobe, entre autres, le respect de l'intégrité physique de la personne (CEDH, grande chambre, 8 avril 2021, *Vavřička e.a. c. République tchèque*, ECLI:CE:ECHR:2021:0408JUD004762113, § 261) et la protection des données à caractère personnel et des informations personnelles relatives à la santé (CEDH, 25 février 1997, *Z. c. Finlande*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; 10 octobre 2006, *L.L. c. France*, ECLI:CE:ECHR:2006:1010JUD000750802, § 32; 27 février 2018, *Mockuté c. Lituanie*, ECLI:CE:ECHR:2018:0227JUD006649009, § 93). La jurisprudence de la Cour européenne des droits de l'homme fait apparaître que de la protection de ce droit relèvent notamment les données et informations personnelles suivantes : le nom, l'adresse, les activités professionnelles, les relations personnelles, les empreintes digitales, les images filmées, les photographies, les communications, les données ADN, les données judiciaires (condamnations ou inculpations), les données financières, les informations concernant des biens et les données médicales (voy. notamment CEDH, 26 mars 1987, *Leander c. Suède*, ECLI:CE:ECHR:1987:0326JUD000924881, §§ 47-48; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, ECLI:CE:ECHR:2008:1204JUD003056204, §§ 66-68; 17 décembre 2009, *B.B. c. France*, ECLI:CE:ECHR:2009:1217JUD000533506, § 57; 10 février 2011, *Dimitrov-Kazakov c. Bulgarie*, ECLI:CE:ECHR:2011:0210JUD001137903, §§ 29-31; 18 octobre 2011, *Khelili c. Suisse*, ECLI:CE:ECHR:2011:1018JUD001618807, §§ 55-57; 9 octobre 2012, *Alkaya c. Turquie*, ECLI:CE:ECHR:2012:1009JUD004281106, § 29; 18 avril 2013, *M.K. c. France*, ECLI:CE:ECHR:2013:0418JUD001952209, § 26; 18 septembre 2014, *Brunet c. France*, ECLI:CE:ECHR:2014:0918JUD002101010, § 31; 13 octobre 2020, *Frâncu c. Roumanie*, ECLI:CE:ECHR:2020:1013JUD006935613, § 51).

La protection des données à caractère personnel relatives à la santé est capitale non seulement pour protéger la vie privée de la personne, mais également pour préserver sa confiance dans les services de santé (CEDH, 25 février 1997, *Z. c. Finlande*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95). Faute d'une telle protection, les personnes pourraient être dissuadées de fournir les informations à caractère personnel et intime nécessaires à la prescription du traitement approprié, ce qui pourrait mettre en danger leur santé voire, dans les cas des maladies transmissibles, celle de la collectivité (*ibid.*, § 95).

B.16.5. Le droit au respect de la vie privée n'est toutefois pas absolu. L'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme n'excluent pas une ingérence d'une autorité publique dans l'exercice de ce droit, pourvu que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit. Ces dispositions engendrent de surcroît l'obligation positive, pour l'autorité publique, de prendre des mesures qui assurent le respect effectif de la vie privée, même dans la sphère des relations entre les individus (CEDH, 27 octobre 1994, *Kroon et autres c. Pays-Bas*, ECLI:CE:ECHR:1994:1027JUD001853591, § 31; grande chambre, 12 novembre 2013, *Söderman c. Suède*, ECLI:CE:ECHR:2013:1112JUD000578608, § 78).

Lorsqu'elles mettent en balance l'intérêt de l'État à traiter des données à caractère personnel et l'intérêt individuel à la protection de la confidentialité de ces données, les autorités nationales disposent d'une certaine marge d'appréciation (*ibid.*, § 99). Eu égard à l'importance fondamentale de la protection des données à caractère personnel, cette marge est toutefois assez limitée (CEDH, 26 janvier 2017, *Surikov c. Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 73). Pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut qu'un juste équilibre soit atteint entre tous les droits et intérêts en cause. Pour juger de cet équilibre, il faut tenir compte notamment des dispositions de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après : la Convention n° 108) (CEDH, 25 février 1997, *Z c. Finlande*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, ECLI:CE:ECHR:2008:1204JUD003056204, § 103; 26 janvier 2017, *Surikov c. Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

La Convention n° 108 contient, entre autres, les principes relatifs au traitement de données à caractère personnel : licéité, loyauté, transparence, limitation des finalités, proportionnalité, exactitude, limitation de la conservation, intégrité et confidentialité, et responsabilité.

La même Convention est actualisée par un protocole d'amendement ouvert à signature le 10 octobre 2018.

Il découle de la Convention n° 108 que le droit national doit notamment garantir que les données à caractère personnel sont pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ou détenues, que les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire et que les données détenues sont protégées efficacement contre les usages impropres et abusifs. Elle a aussi indiqué qu'il est essentiel que le droit national prévoie des règles claires et détaillées relatives à la portée et à l'application des mesures concernées, ainsi que des garanties minimales concernant, entre autres, la durée, la conservation, l'utilisation, l'accès des tiers, les procédures de préservation de l'intégrité et de la confidentialité des données et les procédures de destruction de celles-ci, de sorte qu'il existe suffisamment de garanties contre le risque d'abus et d'arbitraire à chaque étape du traitement des données (CEDH, 26 janvier 2017, *Surikov c. Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

B.16.6. Dans le champ d'application du droit de l'Union européenne, l'article 22 de la Constitution, l'article 8 de la Convention européenne des droits de l'homme et l'article 7 de la Charte garantissent des droits fondamentaux analogues (CJUE, grande chambre, 9 novembre 2010, C-92/09 et C-93/09, *Volker und Markus Schecke GbR e.a.*, ECLI:EU:C:2010:662), alors que l'article 8 de cette Charte vise spécifiquement la protection des données à caractère personnel.

B.16.7. La Cour de justice de l'Union européenne considère que le respect du droit à la vie privée à l'égard du traitement de données à caractère personnel se rapporte à toute information concernant une personne physique identifiée ou identifiable (CJUE, grande chambre, 9 novembre 2010, C-92/09 et C-93/09, *Volker und Markus Schecke GbR e.a,* ECLI:EU:C:2010:662, point 52; 16 janvier 2019, C-496/17, *Deutsche Post AG*, ECLI:EU:C:2019:26, point 54).

B.16.8. Les droits consacrés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne n'apparaissent pas non plus comme étant des prérogatives absolues (CJUE, grande chambre, 16 juillet 2020, C-311/18, *Data Protection Commissioner*, ECLI:EU:C:2020:559, point 172).

Conformément à l'article 52, paragraphe 1, première phrase, de la Charte des droits fondamentaux de l'Union européenne, toute limitation de l'exercice des droits et libertés reconnus par celle-ci, dont notamment le droit au respect de la vie privée garanti par l'article 7 et le droit à la protection des données à caractère personnel consacré par l'article 8, doit être prévue par la loi, respecter le contenu essentiel de ces droits et, dans le respect du principe de proportionnalité, être nécessaire et répondre effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui (CJUE, grande chambre, 6 octobre 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, point 64). Dans le même sens, conformément à l'article 23 du RGPD, les limitations apportées à certaines obligations des responsables du traitement prévues par la Charte des droits fondamentaux de l'Union européenne et aux droits des intéressés doivent être prévues par la loi, respecter l'essence des libertés et des droits fondamentaux et constituer une mesure nécessaire et proportionnée dans une société démocratique pour atteindre le but poursuivi et respecter les dispositions spécifiques contenues au paragraphe 2 (CJUE, grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, ECLI:EU:C:2020:791, points 209-210; 10 décembre 2020, C-620/19, *Land Nordrhein-Westfalen*, ECLI:EU:C:2020:1011, point 46).

B.16.9. L'article 22 de la Constitution réserve au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée. Il garantit ainsi à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et qu'elle porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur.

Par conséquent, les éléments essentiels du traitement des données à caractère personnel doivent être fixés dans la loi, le décret ou l'ordonnance même. À cet égard, quelle que soit la matière concernée, les éléments suivants constituent en principe, des éléments essentiels : (1°) la catégorie de données traitées; (2°) la catégorie de personnes concernées; (3°) la finalité poursuivie par le traitement; (4°) la catégorie de personnes ayant accès aux données traitées et (5°) le délai maximal de conservation des données (avis de l'assemblée générale de la section de législation du Conseil d'État n° 68.936/AG du 7 avril 2021 sur un avant-projet de loi « relative aux mesures de police administrative lors d'une situation d'urgence épidémique », (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1951/001, p. 119).

B.16.10. Outre l'exigence de légalité formelle, l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme et avec les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne, impose que l'ingérence dans l'exercice du droit au respect de la vie privée et du droit à la protection des données à caractère personnel soit définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence.

En matière de protection des données, cette exigence de prévisibilité implique qu'il doit être prévu de manière suffisamment précise dans quelles circonstances les traitements de données à caractère personnel sont autorisés (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, ECLI:CE:ECHR:2000:0504JUD002834195, § 57; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, ECLI:CE:ECHR:2008:1204JUD003056204, § 99). L'exigence selon laquelle la limitation doit être prévue par la loi implique notamment que la base légale qui permet l'ingérence dans ces droits doit elle-même définir la portée de la limitation de l'exercice du droit concerné (CJUE, 6 octobre 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, point 65).

Toute personne doit dès lors pouvoir avoir une idée suffisamment claire des données traitées, des personnes concernées par un traitement de données déterminé et des conditions et finalités dudit traitement.

B.16.11. L'article 5 du RGPD, intitulé « Principes relatifs au traitement », dispose :

« 1. Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité) ».

L'article 6 du RGPD, intitulé « Licéité du traitement », dispose :

« 1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

2. Les États membres peuvent maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement pour ce qui est du traitement dans le but de respecter le paragraphe 1, points c) et e), en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal, y compris dans d'autres situations particulières de traitement comme le prévoit le chapitre IX.

3. Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par :

a) le droit de l'Union; ou

b) le droit de l'État membre auquel le responsable du traitement est soumis.

Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres : les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi.

4. Lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1, le responsable du traitement, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, entre autres :

a) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé;

b) du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement;

c) de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10;

d) des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées;

e) de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation ».

L'article 9 du RGPD, intitulé « Traitement portant sur des catégories particulières de données à caractère personnel », dispose :

« 1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée;

[...]

h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3;

i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel;

[...]

3. Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents.

4. Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé ».

L'article 35 du RGPD, intitulé « Analyse d'impact relative à la protection des données », dispose :

« 1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

2. Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

3. L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants :

a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;

b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou

c) la surveillance systématique à grande échelle d'une zone accessible au public.

4. L'autorité de contrôle établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément au paragraphe 1. L'autorité de contrôle communique ces listes au comité visé à l'article 68.

5. L'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au comité.

6. Avant d'adopter les listes visées aux paragraphes 4 et 5, l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence visé à l'article 63, lorsque ces listes comprennent des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union.

7. L'analyse contient au moins:

a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;

b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;

c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et

d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

8. Le respect, par les responsables du traitement ou sous-traitants concernés, de codes de conduite approuvés visés à l'article 40 est dûment pris en compte lors de l'évaluation de l'impact des opérations de traitement effectuées par lesdits responsables du traitement ou sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données.

9. Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

10. Lorsque le traitement effectué en application de l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.

11. Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement ».

B.16.12. La non-rétroactivité des lois 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, dans une mesure raisonnable, les conséquences d'un acte déterminé au moment où cet acte est accompli. La rétroactivité ne se justifie que si elle est indispensable à la réalisation d'un objectif d'intérêt général.

S'il s'avère que la rétroactivité a en outre pour but ou pour effet d'influencer dans un sens l'issue de procédures judiciaires ou que les juridictions soient empêchées de se prononcer sur une question de droit bien précise, la nature du principe en cause exige que des circonstances exceptionnelles ou des motifs impérieux d'intérêt général justifient l'intervention du législateur, laquelle porte atteinte, au préjudice d'une catégorie de citoyens, aux garanties juridictionnelles offertes à tous.

B.17. Les griefs de la partie requérante portent sur les aspects suivants :

I. les finalités du traitement des données de vaccination, visées à l'article 4, § 2 (première branche) (B.18-B.24);

II. l'habilitation, visée à l'article 5, conférée au Comité de sécurité de l'information d'autoriser la communication de données à caractère personnel à des tiers (première branche) (B.25-B.32);

III. la durée de conservation des données enregistrées dans « Vaccinnet », visée à l'article 6 (deuxième branche) (B.33-B.38);

IV. l'absence d'analyse d'impact préalable requise par l'article 35 du RGPD (deuxième branche) (B.39-B.45);

V. la rétroactivité des effets de l'accord de coopération au 24 décembre 2020, prévue par l'article 12 (troisième branche) (B.46-B.50).

I. En ce qui concerne les finalités du traitement des données de vaccination, visées à l'article 4, § 2 (première branche)

B.18. Dans la première branche du moyen, la partie requérante estime que les onze finalités définies dans l'article 4, § 2, de l'accord de coopération du 12 mars 2021 ne sont pas suffisamment « déterminées et explicites », de sorte que ne sont pas respectés les principes de légalité et de prévisibilité à l'égard d'éléments essentiels du traitement de données sensibles à caractère personnel. Elle critique plus précisément le caractère large de la finalité visée au 1° ainsi que la nécessité de la finalité visée au 11°.

B.19. L'article 4, § 2, de l'accord de coopération du 12 mars 2021 dispose :

« Le traitement des données à caractère personnel visées à l'article 3, § 2, poursuit les finalités de traitement suivantes :

1° la prestation de soins de santé et de traitements, telle que visée à l'article 9, 2, h du Règlement général sur la Protection des données, ce que visent exclusivement l'acte de vaccination et les mesures de soutien, d'information, de sensibilisation des citoyens en rapport avec la vaccination;

2° la pharmacovigilance des vaccins contre la COVID-19, conformément à l'article 12*sexies* de la loi du 25 mars 1964 sur les médicaments et aux lignes directrices détaillées publiées par la Commission européenne dans le ' Module VI - Collecte, gestion et transmission des notifications d'effets indésirables présumés des médicaments (GVP) ', telles qu'elles figurent dans la dernière version disponible, et visées à l'article 4, paragraphe 1, 3° de la loi du 20 juillet 2006 relative à la création et au fonctionnement de l'Agence fédérale des médicaments et des produits de santé;

3° la traçabilité des vaccins contre la COVID-19 afin d'assurer le suivi des ' rapid alerts de vigilance ' et ' rapid alerts de qualité ' visées à l'article 4, paragraphe 1, 3ème alinéa, 3°, e, et 4°, j, de la loi du 20 juillet 2006 relative à la création et au fonctionnement de l'Agence fédérale des médicaments et des produits de santé;

4° la gestion de schémas de vaccinations contre la COVID-19 par personne à vacciner ou vaccinée et la planification des plages de vaccination, notamment par les centres de vaccination;

5° l'organisation logistique de la vaccination contre la COVID-19, après anonymisation des données ou à tout le moins pseudonymisation des données dans l'hypothèse où l'anonymisation ne permettrait pas de réaliser l'organisation logistique;

6° la détermination du taux de vaccination anonyme contre la COVID-19 de la population;

7° l'organisation du suivi des contacts en exécution de l'Accord de coopération du 25 août 2020 entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les services d'inspections d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 se fondant sur une base de données auprès de Sciensano;

8° l'exécution du suivi et de la surveillance post-autorisation des vaccins conformément aux bonnes pratiques recommandées par l'Organisation mondiale de la Santé, après anonymisation des données ou à tout le moins pseudonymisation des données dans l'hypothèse où l'anonymisation ne permettrait pas de réaliser le suivi et la surveillance post-autorisation;

9° sans préjudice de la réglementation relative à l'assurance maladie, le calcul de la répartition des coûts de vaccination entre l'Etat 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;

10° l'exécution d'études scientifiques ou statistiques, conformément à l'article 89, § 1er, du Règlement général sur la protection des données et, le cas échéant, à l'article 89, §§ 2 et 3, du Règlement général sur la protection des données et 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, après anonymisation, ou à tout le moins pseudonymisation, dans l'hypothèse où l'anonymisation ne permettrait pas de réaliser l'étude scientifique ou statistique.

11° l'information et la sensibilisation des personnes concernant la vaccination contre la COVID-19 par les prestataires de soins et les organismes assureurs ».

B.20.1. Concernant les finalités visées à l'article 4, l'exposé général de l'accord de coopération du 12 mars 2021 indique :

« L'article 4 décrit les finalités de traitement par base de données; il s'agit dans l'ensemble des finalités suivantes :

- la prestation des soins de qualité pour la personne concernée, ce que visent exclusivement l'acte de vaccination et les mesures de soutien, d'information, de sensibilisation des citoyens en rapport avec la vaccination;

- la pharmacovigilance;

- la traçabilité des vaccins;

- la gestion de schémas de vaccination contre la COVID-19 et la planification des plages de vaccination, notamment par les centres de vaccination et par les prestataires de soins;

- l'organisation logistique de la vaccination contre la COVID-19; à cet égard, il est utile de préciser que pour atteindre cette finalité, tant la base de données des codes de vaccination que la base de données d'enregistrement des vaccinations sont nécessaires, la seconde permettant notamment d'alimenter la première par exemple afin d'éviter de réinviter des personnes déjà vaccinées ou encore d'identifier les besoins en vaccins ou de personnel médical au regard des vaccinations devant encore être administrées;

- la détermination du taux de vaccination anonyme contre la COVID-19 de la population;

- l'organisation du traçage des contacts;

- l'exécution du suivi et de la surveillance post-autorisation des vaccins;

- le calcul de la répartition des coûts de vaccination entre l'Etat fédéral et les entités fédérées;

- le soutien de la recherche scientifique, notamment en matière d'efficacité et de sécurité des vaccins;

- l'information et la sensibilisation des personnes concernant la vaccination contre la COVID-19 par les services d'inspection d'hygiène des entités fédérées, les prestataires de soins et les organismes assureurs afin d'obtenir un degré de vaccination maximal;

- l'invitation et l'offre d'aide lors du processus d'invitation des personnes à se faire vacciner contre la COVID-19 par les prestataires de soins, les organismes assureurs, les centres de vaccination, l'autorité fédérale, les entités fédérées compétentes et les administrations locales.

Concernant la finalité relative au suivi et à la surveillance post-autorisation des vaccins, il peut être précisé les éléments suivants.

Les études sur l'acceptation et l'utilisation des vaccins et la couverture vaccinale permettent de savoir combien de personnes sont prêtes à se faire vacciner et combien le font effectivement. Plus précisément, les études de couverture vaccinale permettent d'estimer la proportion de personnes vaccinées dans des groupes à risque spécifiques, comme les personnes âgées ou les personnes souffrant de troubles sous-jacents spécifiques. Ces études donneront un aperçu des attitudes de la population à l'égard des vaccins et aideront à identifier les lacunes du programme de vaccination qui doivent être comblées.

Le suivi de l'efficacité, de la séroprévalence et de l'immunogénicité des vaccins permet d'évaluer la capacité du vaccin à induire une réponse immunitaire et à prévenir l'infection à long terme et en cas de nouvelles souches en circulation.

Enfin, il est crucial de surveiller la qualité des vaccins et de mettre en place un système capable de détecter les effets indésirables tardifs ou rares afin de continuer à garantir la sécurité des vaccins.

Dans l'ensemble, les résultats de la surveillance post-autorisation sont utilisés pour orienter la politique en matière de vaccins et pour informer les professionnels de la santé et la population générale des résultats du programme de vaccination COVID-19 de la Belgique.

En tout état de cause, ce suivi et la surveillance post-autorisation des vaccins est organisée conformément aux bonnes pratiques recommandées par l'Organisation mondiale de la Santé en la matière.

Il y a lieu de souligner l'importance du rapport avec le traçage des contacts dès lors qu'une des finalités concerne l'organisation du traçage. Les scénarios visés qui permettent la liaison entre la vaccination et le suivi de contact doit impérativement s'inscrire dans un but exclusif de suivi de contact infectieux et du suivi de la vaccination. Sont notamment envisageables :

- 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 dès lors que le vaccin s'avère être une mesure de prophylaxie efficace;

- les contacts ne sont pas vaccinés, il y a donc lieu de continuer à cartographier activement l'épidémie.

Les données qui sont transmises dans ce cadre à partir de Vaccinnet vers la banque de données de Sciensano concernent a priori le NISS, le statut de vaccination et le type de vaccin, mais une flexibilité s'impose en fonction de l'évolution des connaissances scientifiques en ce qui concerne l'impact de la vaccination sur les risques d'infection.

Par ailleurs, il y a lieu de souligner que les données à caractère personnel sont nécessaires pour assurer le suivi médical du patient en rapport avec la vaccination COVID-19 dès lors qu'une couverture vaccinale importante au sein de la population constitue un enjeu majeur et fondamental de santé publique au regard de la crise pandémique inédite de la COVID-19 ainsi qu'à l'échelle de l'individu qui doit pouvoir réaliser un choix pour sa santé personnelle de manière informée. Ceci requiert, en effet, une combinaison d'informations générales et ciblées (à l'initiative du médecin traitant ou de l'organisme assureur pour leurs propres patients et membres). Il est notamment d'une importance capitale que le médecin (le médecin généraliste, le spécialiste) évalue, sur la base de ses connaissances détaillées de l'anamnèse médicale du patient confié à ses soins, si la vaccination du patient qui a été correctement informé, est ou non importante. Dans ce cadre, il convient de souligner qu'il y a lieu de veiller en permanence à un taux de vaccination suffisant (par exemple, 70 pour cent) et qu'il est important d'assurer un suivi ciblé (via des campagnes et au niveau individuel) à ce niveau. Il va de soi qu'il est interdit de contacter, si elles ne le souhaitent pas, les personnes qui ont explicitement déclaré qu'elles refusent le vaccin.

N'est pas visé dans la finalité relative à la prestation de soins de qualité, le fait de limiter ou de conditionner l'accès à des soins de qualité de quelque manière que ce soit en raison de l'état vaccinal d'une personne.

Il y a ensuite lieu d'observer que le degré de vaccination anonyme contre la COVID-19 doit pouvoir être déterminé de manière granulaire (par exemple dans les centres de soins résidentiels, une distinction doit être opérée entre le personnel soignant et les résidents) et que cette détermination ne peut pas toujours être réalisée au moyen de données anonymes ou à tout le moins pseudonymisées au cas où l'anonymisation ne permettrait pas d'atteindre l'objectif visé.

Par ailleurs, il est utile de préciser que toutes les catégories de données enregistrées à la fois dans la banque de données des codes de vaccination et dans la banque de données d'enregistrement des vaccinations peuvent en principe être traitées et conservées pour chacune des finalités. Le texte de l'accord de coopération précise, par ailleurs, les cas où seules des données anonymes ou à tout le moins pseudonymisées sont concernées, au cas où l'anonymisation ne permettrait pas d'atteindre l'objectif visé.

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.

Les données collectées dans le cadre du présent accord de coopération ne peuvent donc pas être utilisées à d'autres fins que celles prévues par le présent article, notamment mais pas exclusivement à des fins policières, commerciales, fiscales, pénales ou de sécurité de l'Etat.

Finalement, l'utilisation des données des bases de données doit évidemment être conforme à l'article 14 de la Convention européenne des droits de l'homme, aux articles 10 et 11 de la Constitution et à la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination.

Tout utilisateur de soins a le droit d'obtenir une attestation de vaccination. Cette attestation ne peut cependant jamais donner lieu à une discrimination à l'égard des utilisateurs de soins » (*Moniteur belge* du 12 avril 2021, pp. 32404-32408; voy. aussi *Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, pp. 9-13).

B.20.2. Dans son avis sur l'avant-projet de loi devenu la loi du 2 avril 2021 portant assentiment à l'accord de coopération du 12 mars 2021, la section de législation du Conseil d'État a observé, concernant les finalités du traitement de données :

« 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 » (*ibid.*, pp. 51-52; voy. aussi *Doc. parl.*, Parlement flamand, 2020-2021, n° 708/1, p. 88; *Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, p. 84; *Doc. parl.*, Parlement de la Communauté germanophone, 2020-2021, n° 132/1, pp. 31-32; *Doc. parl.*, Assemblée réunie de la Commission communautaire commune, 2020-2021, n° B-65/1, pp. 16-17; *Doc. parl.*, Assemblée de la Commission communautaire française, 2020-2021, n° 45/1, p. 32).

B.20.3. Dans son avis n° 16/2021 du 10 février 2021, relatif au projet d'accord de coopération devenu l'accord de coopération du 12 mars 2021, l'Autorité de protection des données a observé :

« 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. Le ministre de la Santé publique a précisé que « l'accord de coopération ne concerne que la campagne de vaccination contre le COVID-19 et que les données ne peuvent pas être utilisées pour d'autres finalités », que celles qui « concernent exclusivement la campagne de vaccination » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/002, p. 12).

B.21.1. En vertu du principe de la minimisation des données, les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (article 5, paragraphe 1, point c), du RGPD).

B.21.2. Comme il est dit en B.16.4, le droit au respect de la vie privée englobe la protection des données à caractère personnel et des informations personnelles dont relèvent, notamment, le nom et les données de santé.

Les actes attaqués, qui portent assentiment à des dispositions qui prévoient le traitement des données à caractère personnel, y compris des données sensibles sur la santé, dans la banque de données « Vaccinnet », entraînent une ingérence dans le droit à la protection des données à caractère personnel, garanti par les dispositions citées en B.16.

L'article 4, paragraphe 15, du RGPD définit les « données concernant la santé », comme « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ». Dès lors que les données enregistrées dans la banque de données « Vaccinnet » portent notamment sur des données concernant la santé au sens de la disposition précitée, elles doivent être traitées conformément à l'article 9 du RGPD.

L'article 9, paragraphe 1, du RGPD interdit en principe le traitement de données à caractère personnel sensibles, telles les données concernant la santé. L'article 9, paragraphe 2, point h), du RGPD permet toutefois un tel traitement lorsqu'il est nécessaire « aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé » et qu'il est soumis à une obligation de secret professionnel. L'article 9, paragraphe 2, point i), du RGPD prévoit que le traitement de telles données est également autorisé lorsqu'il est nécessaire « pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ».

Le considérant 54 du RGPD énonce à cet égard :

« Le traitement des catégories particulières de données à caractère personnel peut être nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique, sans le consentement de la personne concernée. Un tel traitement devrait faire l'objet de mesures appropriées et spécifiques de façon à protéger les droits et libertés des personnes physiques. Dans ce contexte, la notion de ' santé publique ' devrait s'interpréter selon la définition contenue dans le règlement (CE) n° 1338/2008 du Parlement européen et du Conseil, à savoir tous les éléments relatifs à la santé, à savoir l'état de santé, morbidité et handicap inclus, les déterminants ayant un effet sur cet état de santé, les besoins en matière de soins de santé, les ressources consacrées aux soins de santé, la fourniture de soins de santé, l'accès universel à ces soins, les dépenses de santé et leur financement, ainsi que les causes de mortalité. De tels traitements de données concernant la santé pour des motifs d'intérêt public ne devraient pas aboutir à ce que des données à caractère personnel soient traitées à d'autres fins par des tiers, tels que les employeurs ou les compagnies d'assurance et les banques ».

B.21.3. En vertu du principe de la limitation des finalités, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et le traitement ultérieur éventuel de ces données doit être compatible avec ces finalités initiales (article 5, paragraphe 1, point b), du RGPD).

Comme il est dit en B.16.9 et B.16.10, en vertu du principe de légalité, toute personne doit avoir une idée suffisamment claire des finalités du traitement des données qui la concernent.

B.22.1. Les actes attaqués poursuivent un objectif légitime de lutte contre la propagation du coronavirus SARS-CoV-2, qui est un virus aéroporté très contagieux. La pandémie de COVID-19 se caractérise par un taux de reproduction élevé. Si des mesures sanitaires ne sont pas prises, ce virus se propage très rapidement, de manière exponentielle.

Comme il est dit en B.2, l'enregistrement des données de vaccination s'inscrit, d'une part, dans la stratégie de vaccination belge établie sur la base des données scientifiques en matière de vaccins contre la COVID-19, telles qu'elles étaient disponibles au moment de l'adoption des actes attaqués, afin de lutter contre la pandémie de COVID-19 en diminuant les contaminations liées au coronavirus COVID-19, ainsi que, d'autre part, dans la mise en œuvre au niveau européen d'un certificat COVID numérique de l'UE, basé sur le souci d'interopérabilité, entre autres, des certificats de vaccination.

Dans ce contexte, l'enregistrement des données de vaccination est indispensable à la poursuite de ces objectifs, et la centralisation de l'enregistrement de ces données permet d'« identifier le schéma posologique adéquat, notamment en ce qui concerne les différentes doses d'un vaccin à administrer (intervalle optimal proposé en cas de vaccins multi-doses) et vise à assurer le bon fonctionnement de la campagne [de] vaccination massive contre la COVID-19 » (*Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, p. 3).

Une telle mesure vise dès lors à garantir la santé d'autrui et la santé publique, ainsi que les droits et libertés d'autrui.

B.22.2. L'accord de coopération du 12 mars 2021 identifie expressément, dans ce contexte, onze finalités pour lesquelles les données à caractère personnel mentionnées dans l'article 3, § 2, sont collectées et traitées dans la banque de données « Vaccinnet », et l'exposé général de l'accord de coopération du 12 mars 2021 précise expressément que ces données « ne peuvent être utilisées à d'autres fins que celles prévues dans le présent accord », « notamment mais pas exclusivement à des fins policières, commerciales, fiscales, pénales ou de sécurité de l'Etat » (*Moniteur belge* du 12 avril 2021, p. 32407).

En adoptant les actes attaqués, les différents législateurs compétents ont réglé eux-mêmes les éléments essentiels du traitement des données à caractère personnel, conformément à ce qui est dit en B.16.9 et B.16.10, en définissant de manière exhaustive les finalités du traitement des données figurant dans la banque de données « Vaccinnet ».

Par ailleurs, l'exposé général de l'accord de coopération du 12 mars 2021 apporte de nombreuses précisions quant aux finalités, répondant ainsi aux critiques formulées par l'Autorité de protection des données dans son avis cité en B.20.3.

B.23.1. Pour examiner le caractère déterminé des finalités visées à l'article 4, § 2, de l'accord de coopération, la Cour doit, dans le contexte rappelé en B.2, prendre en compte le caractère intrinsèquement évolutif des connaissances scientifiques relatives aux spécificités du coronavirus SARS-CoV-2 et de ses possibles mutations, mais aussi à l'efficacité des vaccins mis sur le marché peu de temps avant le lancement de la campagne de vaccination et leur efficacité à moyen et long terme.

B.23.2.1. Il ressort des travaux préparatoires cités en B.20 que les onze finalités définies dans l'article 4, § 2, sont directement liées à la campagne de vaccination massive, déployée au niveau national, menée sur la base des connaissances scientifiques disponibles au moment du lancement de cette campagne.

Le seul fait que les finalités d'un traitement de données soient au nombre de onze ne permet pas, comme le soutient la partie requérante, de conclure que ces finalités seraient, en soi, excessives. En effet, le caractère déterminé d'une finalité doit s'apprécier en fonction des circonstances d'espèce et l'explicitation des différentes finalités peut constituer une garantie pour le traitement des données (opinion 03/2013 sur la limitation des finalités, 2 avril 2013, Groupe de travail « Article 29 » sur la protection des données, p. 15).

B.23.2.2. Ainsi, les finalités de « pharmacovigilance des vaccins contre la COVID-19 » (2°), de « traçabilité des vaccins » (3°), de « gestion des schémas de vaccinations » (4°), d'« organisation logistique de la vaccination contre la COVID-19 » (5°), de « détermination du taux de vaccination anonyme contre la COVID-19 de la population » (6°) et d'« exécution du suivi et de la surveillance post-autorisation des vaccins » (8°) sont précises et directement liées à l'organisation de la campagne de vaccination massive contre la COVID-19, menée au niveau national.

Ces différents éléments sont en effet nécessaires pour mettre en œuvre l'organisation logistique de la vaccination, compte tenu des différents groupes cibles à inviter et du nombre de doses à administrer, mais aussi pour évaluer le taux de couverture vaccinale, la capacité du vaccin à induire une réponse immunitaire et pour détecter les éventuels effets indésirables de ce vaccin. Le suivi et la surveillance post-autorisation des vaccins sont organisés conformément aux bonnes pratiques de l'Organisation mondiale de la santé en la matière. Dans le cadre de la finalité de « pharmacovigilance des vaccins », l'article 45 de la loi du 13 juin 2021 « portant des mesures de gestion de la pandémie COVID-19 et d'autres mesures urgentes dans le domaine des soins de santé » prévoit l'intégration de données figurant dans « Vaccinnet » dans une base de données fédérale, dont le responsable du traitement est l'Agence fédérale des médicaments et des produits de santé.

Contrairement à ce que la partie requérante allègue, la finalité relative à la « prestation de soins de santé et de traitements » a été expressément limitée dans l'article 4, § 2, 1°, de l'accord de coopération du 12 mars 2021 comme visant « exclusivement l'acte de vaccination et les mesures de soutien, d'information, de sensibilisation des citoyens en rapport avec la vaccination », en référence à l'article 9, paragraphe 2, point h), du RGPD. Il a également été précisé que cette finalité ne porte aucunement sur « le fait de limiter ou de conditionner l'accès à des soins de qualité de quelque manière que ce soit en raison de l'état vaccinal d'une personne » (exposé général de l'accord de coopération du 12 mars 2021, *Moniteur belge* du 12 avril 2021, p. 32407). Il en résulte que cette finalité est également précise et directement liée à la vaccination contre la COVID-19 et au suivi médical de la personne vaccinée.

La finalité visée à l'article 4, § 2, 1°, est ainsi également liée à la finalité d'« exécution d'études scientifiques ou statistiques » visée à l'article 4, § 2, 10°, ainsi qu'à la finalité relative à « l'information et la sensibilisation des personnes concernant la vaccination contre la COVID-19 » visée à l'article 4, § 2, 11°. Il ressort en effet des principes décidés en matière de stratégie de vaccination que la Belgique tend à atteindre une forme d'immunité collective par un taux de vaccination suffisant de 70 % de la population. Le traitement des données à des fins de recherche scientifique et statistique est notamment visé par l'article 89, paragraphe 1, du RGPD, qui prévoit le principe de minimisation des données, notamment la pseudonymisation qui est, à tout le moins prévue dans l'article 4, § 2, 10°, dans l'hypothèse où l'anonymisation ne permettrait pas de réaliser l'étude scientifique ou statistique. Il a été souligné à cet égard qu'une « couverture vaccinale importante au sein de la population constitue un enjeu majeur et fondamental de santé publique au regard de la crise pandémique inédite de la COVID-19 ainsi qu'à l'échelle de l'individu qui doit pouvoir réaliser un choix pour sa santé personnelle de manière informée » (exposé général de l'accord de coopération du 12 mars 2021, *Moniteur belge* du 12 avril 2021, p. 32407), de sorte que des études statistiques sur cette couverture vaccinale sont nécessaires. Des études sur la couverture vaccinale permettent d'estimer le pourcentage de personnes vaccinées dans les groupes à risques spécifiques et aident à estimer d'éventuelles lacunes du programme de vaccination qui devraient être comblées, le cas échéant par une information et une sensibilisation ciblées, au moyen de campagnes générales ou au niveau individuel, en fonction des attitudes constatées au sein de la population. Le fait que la vaccination s'opère sur une base volontaire rend, dans ce contexte, la finalité d'information et de sensibilisation nécessaire, au regard de l'objectif d'atteindre une couverture vaccinale suffisante. Sur la base de ces connaissances, le rôle du médecin dans cette information ciblée peut se révéler important, même s'il est interdit de contacter des personnes qui ont explicitement déclaré qu'elles refusent le vaccin (*ibid.*).

B.23.2.3. La finalité relative au « traçage des contacts » (7°) est liée au fait que, dans le but exclusif du suivi des contacts infectieux, le statut vaccinal influence directement le risque de contamination. Les données transmises dans ce cadre de « Vaccinnet » vers la banque de données de Sciensano sont limitées, mais « une flexibilité s'impose en fonction de l'évolution des connaissances scientifiques en ce qui concerne l'impact de la vaccination sur les risques d'infection » (*ibid.*, p. 32406).

B.23.2.4. La finalité relative au « calcul de la répartition du coût de vaccination » (9°) entre l'autorité fédérale et les entités fédérées est liée au fait que la campagne de vaccination, gratuite, a été organisée par le biais d'un accord de coopération entre les autorités compétentes, et que les parties à cet accord doivent financer cette vaccination.

Le fait que, comme le souligne la section de législation du Conseil d'État, il est possible que les données ne soient pas anonymisées mais seulement pseudonymisées peut se justifier, comme l'indique l'exposé général de l'accord de coopération à l'égard du degré de vaccination anonyme contre la COVID-19 par le fait que l'anonymisation est susceptible de ne pas permettre d'atteindre l'objectif poursuivi (*ibid.*, p. 32407), mais l'article 4, § 2, 8° garantit que les données concernées seront, à tout le moins, pseudonymisées. Sur la base de cette finalité, le protocole d'accord du 9 février 2022 conclu entre le Gouvernement fédéral et les autorités visées aux articles 128, 130 et 135 de la Constitution « concernant le cofinancement du programme de vaccination contre la COVID-19 » a réparti le coût de la vaccination contre la COVID-19 entre les différentes autorités.

Quant à l'anonymisation ou à la pseudonymisation, il convient de constater qu'il s'agit là de mesures techniques et organisationnelles à adopter pour protéger le traitement des données à caractère personnel, mais qui garantissent toutes deux que l'identité de la personne concernée ne sera pas révélée. Certains éléments peuvent en effet devoir être déterminés de manière « granulaire » : l'exposé général de l'accord de coopération du 12 mars 2021 évoque à cet égard l'exemple des centres de soins résidentiels, dans lesquels une distinction doit être opérée entre le personnel soignant et les résidents (*ibid.*, p. 32407). L'évolution des circonstances et de la réalité épidémiologique peut en effet exiger que la situation soit réglée par une mesure plutôt que par l'autre, sans que la possibilité de recourir à une des deux mesures puisse être considérée comme une absence de détermination quant à un élément essentiel des finalités du traitement des données.

B.23.3. Il résulte de ce qui précède que les finalités définies dans l'article 4, § 2, de l'accord de coopération ont un lien direct avec la campagne de vaccination massive menée au niveau national, sont suffisamment précises et déterminées et sont limitées au strict nécessaire en ce qui concerne cette vaccination.

B.24. En ce qu'il est dirigé contre les actes attaqués en ce qu'ils portent assentiment à l'article 4, § 2, de l'accord de coopération, le moyen unique, dans sa première branche, n'est pas fondé.

II. En ce qui concerne l'habilitation, visée à l'article 5, conférée au Comité de sécurité de l'information d'autoriser la communication de données à caractère personnel à des tiers (première branche)

B.25.1. Dans la première branche du moyen, la partie requérante estime que les catégories de destinataires des données à caractère personnel fixées dans l'article 5 de l'accord de coopération du 12 mars 2021 ne présentent pas de garanties suffisantes de prévisibilité. En outre, l'article 5, alinéa 3, de l'accord de coopération du 12 mars 2021 délègue au Comité de sécurité de l'information la compétence de déterminer des éléments essentiels que sont les instances tierces pouvant traiter les données collectées et ainsi que les finalités du traitement de ces données.

B.25.2. Comme il est dit en B.10.1, les griefs de la partie requérante ne concernent que la banque de données « Vaccinnet », de sorte que la Cour n'examine le moyen dirigé contre l'article 5 de l'accord de coopération du 12 mars 2021 qu'en ce qu'il concerne la communication des données visées à l'article 3, § 2, de l'accord de coopération précité, enregistrées dans la banque de données « Vaccinnet ».

B.26.1. L'article 5 de l'accord de coopération du 12 mars 2021 dispose :

« Dans le but exclusif d'atteindre les finalités listées à l'article 4, les données à caractère personnel visées à l'article 3 peuvent être communiquées à des personnes ou des instances chargées d'une mission d'intérêt public par ou en vertu d'une loi, d'un décret ou d'une ordonnance, à condition que cette communication soit nécessaire à l'exécution de la mission d'intérêt public des personnes ou des instances en question et que seules les données pertinentes au vu des finalités de l'article 4 soient communiquées.

Les données à caractère personnel visées à l'article 3 sont communiquées à des institutions de recherche si elles sont nécessaires pour la réalisation d'études scientifiques ou statistiques, après anonymisation ou à tout le moins pseudonymisation lorsque l'anonymisation ne permettrait pas de réaliser l'étude scientifique ou statistique.

Toute communication des données fait l'objet d'une délibération de la chambre ' sécurité sociale et santé ' du comité de sécurité de l'information, afin de vérifier le respect des conditions énoncées au présent article.

Le Comité de sécurité de l'information publie sur le portail eSanté une description fonctionnelle précise des systèmes d'information mis en place pour la mise en œuvre du présent accord de coopération et des flux d'informations entre ces systèmes d'information qui ont fait l'objet d'une délibération du Comité de sécurité de l'information, en particulier en ce qui concerne le traitement des informations, les processus et les banques de données.

Les délibérations du Comité de sécurité de l'information sont systématiquement publiées sur le site web de la Plate-forme eHealth ».

B.26.2. Concernant la communication des données à des tiers, visée à l'article 5, l'exposé général de l'accord de coopération du 12 mars 2021 indique :

« Dans le but exclusif d'atteindre les finalités listées à l'article 4, les données à caractère personnel visées à l'article 3 peuvent être communiquées à des personnes ou des instances chargées d'une mission d'intérêt public par ou en vertu d'une loi, d'un décret ou d'une ordonnance, à condition que cette communication soit nécessaire à l'exécution de la mission d'intérêt public des personnes ou des instances en question et que seules les données pertinentes au vu des finalités de l'article 4 soient communiquées.

Les données à caractère personnel visées à l'article 3 sont communiquées après anonymisation ou, à tout le moins pseudonymisation, à des institutions de recherche si elles sont nécessaires pour la réalisation d'études scientifiques ou statistiques.(terminologie de l'article 89 du Règlement général sur la protection des données).

Toute communication des données fait l'objet d'une délibération de la chambre ' sécurité sociale et santé ' du comité de sécurité de l'information, afin de vérifier le respect des conditions énoncées au présent article.

Le Comité de sécurité de l'information peut uniquement délibérer pour des échanges de données concrets dans le cadre du présent accord de coopération et ne peut donc, en aucun cas, déterminer d'autres finalités de traitement, ni catégories de données à caractère personnel. Il n'est en aucun cas compétent pour déterminer un élément essentiel du traitement de données à caractère personnel, conformément au principe de légalité tel que prévu à l'article 22 de la Constitution. Il n'est donc pas chargé d'une telle mission sur base du présent accord de coopération.

Le Comité de sécurité de l'information publie sur le portail eSanté une description fonctionnelle précise des systèmes d'information mis en place pour la mise en œuvre du présent accord et des flux d'informations entre ces systèmes d'information qui ont fait l'objet d'une délibération du Comité de sécurité de l'information, en particulier concernant les traitements des informations, les processus et les banques de données.

En outre, les délibérations du Comité de sécurité de l'information sont systématiquement publiées sur le site web de la Plate-forme eHealth. Les délibérations du Comité de sécurité de l'information comprennent toujours les différents aspects nécessaires à l'évaluation du respect de la réglementation relative à la protection de la vie privée lors du traitement de données à caractère personnel (en particulier le Règlement général sur la protection des données). Ainsi, les parties concernées (responsables du traitement) sont toujours explicitement mentionnées, ainsi que les finalités visées et un aperçu (généralement exhaustif) des données à caractère personnel à traiter pour ces finalités. Le Comité de sécurité de l'information vérifie notamment si le traitement de données à caractère personnel est légitime (et répond dès lors à une des conditions mentionnées à l'article 6 du RGPD) et si les principes de base sont respectés (limitation de la finalité, minimisation des données, limitation de la conservation et sécurité de l'information).

L'utilisation d'une base de données commune n'exclut pas que différentes interfaces utilisateur final, éventuellement spécifiques à une entité fédérée, soient utilisées pour alimenter ou consulter la base de données commune.

Il est fondamental de préciser que les données collectées sur base du présent accord de coopération ne peuvent être communiquées que dans deux cas de figure énoncés de manière strictement limitative :

- soit le tiers est, de manière cumulative, chargé d'une mission d'intérêt public et est habilité à traiter de telles données par ou en vertu d'une loi, d'un décret ou d'une ordonnance qui vise expressément une finalité prévue par le présent accord;

- soit le tiers est une institution de recherche pour la réalisation d'études scientifiques ou statistiques. Dans ce cas, sont uniquement communiquées les données anonymisées ou pseudonymisées lorsque l'anonymisation ne permet pas de rencontrer le but poursuivi.

Par tiers il y a lieu d'entendre notamment les prestataires de soins qui ont une relation thérapeutique avec l'utilisateur de soins et les organismes assureurs, dans les limites évidemment de leurs missions respectives.

S'il n'est pas possible ni pertinent de désigner nommément qui sont ces tiers dans un accord de coopération, ces critères permettent néanmoins d'encadrer et de limiter de manière stricte les catégories de tiers concernés. En outre, le rôle du Comité de sécurité de l'information vise à intégrer un filtre supplémentaire afin d'assurer que le flux de données s'inscrit bien dans l'objectif poursuivi et dans la volonté de limiter au maximum la communication de telles données. Ce faisant, il permet d'offrir une flexibilité nécessaire (en ne figeant pas des flux de données évolutives par exemple) et ne peut que renforcer les garanties offertes en matière de vie privée par un contrôle factuel. En effet, il permet d'éviter qu'un flux automatique soit généré sans que ne soit vérifié au préalable qu'il est effectivement permis. Comme le souligne l'Autorité de protection des données dans son avis 16-2021 du 18 février 2021, une délibération du Comité de sécurité de l'information permet également d'apporter une plus-value en précisant davantage les modalités d'exécution, notamment au niveau de la sécurité de l'information et la proportionnalité envisagée par la loi.

En réponse à l'avis du Conseil d'Etat 68/844/VR du 18 février 2021, et au regard de ce qui précède, il convient de préciser que la soumission de la communication de données à caractère personnel à une délibération du Comité de sécurité de l'information est une règle établie par la loi fédérale et constitue une mesure de protection des données dès la conception et par défaut au sens du Règlement Général sur la Protection des Données. Elle est basée sur les articles 6, § 2, et 9, § 4 du Règlement Général sur la Protection des Données.

En effet, les délibérations du Comité de sécurité de l'information précisent les mesures de sécurité de l'information que doivent respecter les acteurs d'une communication de données et évaluent de manière préventive s'il n'y a pas plus de données à caractère personnel qui sont communiquées à l'organisme acquéreur que celles qui lui sont strictement nécessaires pour atteindre des finalités de traitement légitimes.

Les délibérations du Comité de sécurité de l'information sont contraignantes pour les acteurs de l'échange de données. D'autre part, elles visent à offrir une sécurité juridique aux acteurs de l'échange de données afin qu'un partage efficace et efficient des données ne soit pas inutilement hypothéqué par un manque de clarté concernant les mesures de sécurité de l'information à implémenter ou concernant la légitimité de la communication des données à caractère personnel.

Les délibérations du Comité de sécurité de l'information ne portent que sur l'échange (électronique) de données. Dans ses délibérations, le Comité de sécurité de l'information est lié par les dispositions légales régissant les finalités du traitement par les autorités qui reçoivent les données. Les délibérations du Comité de sécurité de l'information ne constituent qu'une base juridique permettant à un organisme traitant des données à caractère personnel sur la base de finalités légitimes de communiquer ces données à caractère personnel à d'autres organismes, dans le cadre des finalités légitimes pour lesquelles l'organisme destinataire peut lui-même traiter ces données à caractère personnel.

Les délibérations du Comité de sécurité de l'information ne constituent pas une base juridique pour la première collecte et le premier traitement de données à caractère personnel par l'organisme émetteur. L'organisme destinataire doit, également, traiter les données à caractère personnel en vertu des bases juridiques dont il dispose. Par conséquent, le Comité de sécurité de l'information ne peut pas étendre les finalités du traitement initial par l'instance qui fournit les données, ni offrir une base juridique pour des finalités de traitement par l'instance destinatrice autres que celles qui sont prévues par ou en vertu d'une loi. Les délibérations autorisent l'échange de données moyennant le respect des modalités décrites dans la délibération sur le plan de la sécurité de l'information et le respect du principe de proportionnalité, mais ne l'imposent pas.

Le Comité de sécurité de l'information n'est pas une autorité de contrôle au sens du Règlement Général sur la Protection des Données. Il n'est donc pas compétent pour contrôler le respect des règles, pour résoudre des problèmes et des litiges ou pour traiter des plaintes. En effet, c'est l'Autorité de protection des données qui est compétente pour ces questions. L'Autorité de protection des données peut à tout moment comparer toute délibération du Comité de sécurité de l'information avec des normes juridiques supérieures et, en cas de non-conformité, demander au Comité de sécurité de l'information de reconsidérer sa délibération sur les points qu'elle a soulevés.

Ce recours au Comité de sécurité de l'information ne se conçoit donc dès lors pas pour les parties prenantes au présent accord de coopération comme un abandon de compétence de par le fait d'une application des règles » (*Moniteur belge* du 12 avril 2021, pp. 32408-32411; voy. aussi *Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, pp. 13-16).

B.27.1. Dans son avis sur l'avant-projet de loi devenue la loi du 2 avril 2021 portant assentiment à l'accord de coopération du 12 mars 2021, la section de législation du Conseil d'État a observé :

« 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 » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, p. 45; voy. aussi *Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, p. 81).

Pour autant qu'il entre dans l'intention des auteurs de l'accord de coopération de maintenir un pouvoir réglementaire au profit de la chambre « sécurité sociale et santé » du Comité de sécurité de l'information, la section de législation du Conseil d'État renvoie à l'observation formulée par l'avis 67.719 du 15 juillet 2020 sur un avant-projet devenu la loi du 9 octobre 2020 « portant assentiment à l'accord de coopération du 25 août 2020 entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les services d'inspection d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 se fondant sur une base de données auprès de Sciensano », au sujet des compétences (réglementaires) qui avaient été déléguées à la chambre « sécurité sociale et santé » du Comité de sécurité de l'information :

« 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 » (*ibid.*, pp. 52-54; voy. aussi *Doc. parl.*, Parlement flamand, 2020-2021, n° 708/1, pp. 88-89; *Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, p. 85; *Doc. parl.*, Parlement de la Communauté germanophone, 2020-2021, n° 132/1, pp. 32-33; *Doc. parl.*, Assemblée réunie de la Commission communautaire commune, 2020-2021, n° B-65/1, pp. 17-18; *Doc. parl.*, Assemblée de la Commission communautaire française, 2020-2021, n° 45/1, p. 33).

B.27.2. Dans son avis n° 16/2021 du 10 février 2021 sur l'avant-projet d'accord de coopération devenu l'accord de coopération du 12 mars 2021, l'Autorité de protection des données a observé :

« 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. Le ministre de la Santé publique a précisé à ce sujet que « la tâche du comité de sécurité de l'information est strictement délimitée. Il ne pourra délibérer que sur les communications de données ayant lieu dans le cadre de cet accord de coopération. Ce comité ne pourra en aucun cas définir lui-même d'autres finalités ou d'autres catégories de données personnelles » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/002, p. 13).

La ministre wallonne de la Santé a aussi précisé que « seuls les tiers qui sont chargés d'une mission publique et qui sont légalement habilités à traiter les données à caractère personnel peuvent recevoir les données » (*Doc. parl.*, Parlement wallon, C.R.I., n° 25, 2020-2021, 31 mars 2021, p. 73).

B.28. En ce qui concerne les données à caractère personnel figurant dans la banque de données « Vaccinnet », l'article 5 de l'accord de coopération définit deux catégories de tiers auxquels ces données peuvent être communiquées : d'une part, « des personnes ou des instances chargées d'une mission d'intérêt public par ou en vertu d'une loi, d'un décret ou d'une ordonnance », auxquelles peuvent être communiquées, parmi les données visées à l'article 3, § 2, seules les données pertinentes au regard des finalités de l'article 4, § 2, et uniquement si cette communication est nécessaire à l'exécution de la mission d'intérêt public de ces personnes ou instances; d'autre part, des « institutions de recherche » si les données sont nécessaires pour réaliser des études scientifiques ou statistiques, après anonymisation ou, à tout le moins, pseudonymisation lorsque l'anonymisation ne permettrait pas de réaliser l'étude scientifique ou statistique.

L'article 5, alinéa 3, subordonne cependant la communication de ces données à caractère personnel à une délibération de la « chambre sécurité sociale et santé » du Comité de sécurité de l'information, aux fins de vérifier le respect des conditions énoncées dans cet article.

B.29.1. Comme il est dit en B.16.9 et B.16.10, en réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée et familiale, l'article 22 de la Constitution garantit à tout citoyen qu'aucune ingérence dans ce droit ne pourra avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

Une délégation à un autre pouvoir n'est pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur.

B.29.2. L'article 6, paragraphe 2, du RGPD dispose que les États membres peuvent maintenir ou introduire des « dispositions plus spécifiques » pour adapter l'application des règles du RGPD en ce qui concerne le traitement nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis (article 6, paragraphe 1, point c)) et le traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement (article 6, paragraphe 1, point e)). L'article 9, paragraphe 2, point h), du RGPD permet le traitement de données sensibles aux fins de la médecine préventive, entouré de différentes garanties, notamment le secret professionnel. L'article 9, paragraphe 2, point i), du RGPD prévoit que le droit de l'Union ou le droit de l'État membre en vertu duquel le traitement de données sensibles est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique prévoit des « mesures appropriées et spécifiques » pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel. L'article 9, paragraphe 4, prévoit que les États membres peuvent maintenir ou introduire des « conditions supplémentaires, y compris des limitations » en ce qui concerne notamment le traitement des données concernant la santé.

B.30.1. Le Comité de sécurité de l'information a été créé par l'article 2, § 1er, de la loi du 5 septembre 2018 « instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE » (ci-après : la loi du 5 septembre 2018). Contrairement aux comités sectoriels supprimés par la loi du 3 décembre 2017 « portant création de l'Autorité de protection des données » auxquels il succède et qui étaient intégrés au sein de l'ancienne Commission de protection de la vie privée, le Comité de sécurité de l'information a été institué comme un nouvel organe indépendant de l'Autorité de protection des données sur pied de l'article 6, paragraphe 2, et de l'article 9, paragraphe 4, précités, du RGPD (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3185/001, pp. 6-7 et 30; DOC 54-3185/005, pp. 7-10). Il ressort des travaux préparatoires de la loi du 5 septembre 2018 que le législateur a voulu que le Comité de sécurité de l'information ne soit considéré ni comme un responsable du traitement, ni comme une autorité de contrôle au sens du RGPD (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3185/001, pp. 8-10).

Conformément à l'article 2, § 2, de la loi du 5 septembre 2018, le Comité de sécurité de l'information est constitué de deux chambres : une chambre « sécurité sociale et santé » et une chambre « autorité fédérale ». Les articles 2, § 1er, et 4, § 1er, alinéa 1er, de la même loi disposent que ses membres sont nommés pour un terme de six ans renouvelable par la Chambre des représentants, qui peut aussi les décharger de leur mission. L'article 5 de la même loi dispose que les membres du Comité de sécurité de l'information « ne reçoivent d'instructions de personne ». Il ressort des travaux préparatoires que le législateur a voulu soustraire le Comité de sécurité de l'information à tout contrôle hiérarchique (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3185/001, p. 10).

Le pouvoir de prendre des décisions administratives qui est confié à la chambre « sécurité sociale et santé » du Comité de sécurité de l'information par l'article 5 de l'accord de coopération du 12 mars 2021 (autoriser ou refuser la communication de données à caractère personnel) est analogue à celui qui est confié à cette chambre par l'article 15, § 1er, alinéa 1er, de la loi du 15 janvier 1990 « relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale », remplacé par l'article 18 de la loi du 5 septembre 2018, par l'article 42, § 2, 3°, de la loi du 13 décembre 2006 « portant dispositions diverses en matière de santé », tel qu'il a été modifié par l'article 43 de la loi du 5 septembre 2018, et par l'article 11 de la loi du 21 août 2008 « relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions », tel qu'il a été modifié par l'article 50 de la loi du 5 septembre 2018. Ces dispositions habilitent la chambre « sécurité sociale et santé » du Comité de sécurité de l'information à autoriser, respectivement, (1) la communication de données sociales à caractère personnel par la Banque-carrefour de la sécurité sociale ou par une institution de sécurité sociale à destination d'une autre institution de sécurité sociale ou d'une instance autre qu'un service public fédéral, un service public de programmation ou un organisme fédéral d'intérêt public, (2) la communication de données à caractère personnel relatives à la santé et (3) la communication de données à caractère personnel par ou à destination de la plate-forme eHealth. Dans l'exercice de leur compétence d'autorisation, les chambres du Comité de sécurité de l'information se limitent à vérifier que la communication de données à caractère personnel concernée respecte les principes de limitation des finalités, de proportionnalité et de sécurité définis par le RGPD (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3185/001, pp. 6, 8 et 9).

L'article 46, § 2, alinéa 1er, de la loi du 15 janvier 1990 « relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale », remplacé par l'article 39 de la loi du 5 septembre 2018, dispose que les délibérations du Comité de sécurité de l'information ont « une portée générale contraignante entre les parties et envers les tiers ». Selon les travaux préparatoires de la loi du 5 septembre 2018, ces délibérations « ont valeur normative (loi au sens matériel), conformément à l'ordre constitutionnel et peuvent être contestées par les voies de recours en vigueur si elles sont contraires aux normes juridiques supérieures » (*ibid.*, p. 8). L'alinéa 2 de la même disposition, dispose :

« L'Autorité de protection des données peut, à tout moment, confronter toute délibération du comité de sécurité de l'information aux normes juridiques supérieures, quel que soit le moment où elle a été rendue. Sans préjudice de ses autres compétences, elle peut demander au comité de sécurité de l'information, lorsqu'elle constate de manière motivée qu'une délibération n'est pas conforme à une norme juridique supérieure, de reconsidérer cette délibération sur les points qu'elle a indiqués, dans un délai de quarante-cinq jours et exclusivement pour le futur. Le cas échéant, le comité de sécurité de l'information soumet la délibération modifiée pour avis à l'Autorité de protection des données. Dans la mesure où cette dernière ne formule pas de remarques supplémentaires dans un délai de quarante-cinq jours, la délibération modifiée est censée être définitive ».

L'article 46, § 1er, 8°, de la loi du 15 janvier 1990 « relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale », remplacé par l'article 39 de la loi du 5 septembre 2018, dispose par ailleurs que le Comité de sécurité de l'information publie chaque année sur le site internet de la Banque-carrefour et sur le site internet de la Plate-forme eHealth un rapport sommaire de l'accomplissement de ses missions au cours de l'année écoulée. Les travaux préparatoires de la loi du 5 septembre 2018 mentionnent enfin que les délibérations du Comité de sécurité de l'information peuvent faire l'objet d'un recours devant le Conseil d'État (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3185/001, pp. 10 et 31).

B.30.2. Il ressort de ce qui précède que, comme la Cour l'a jugé par son arrêt n° 110/2022 du 22 septembre 2022 (ECLI:BE:GHCC:2022:ARR.110), les délibérations du Comité de sécurité de l'information ont une portée contraignante notamment pour les personnes dont le traitement des données personnelles est autorisé par ce Comité. Ces délibérations sont soumises à un contrôle faible de la part de l'Autorité de protection des données puisque celle-ci peut uniquement demander au Comité de sécurité de l'information de « reconsidérer » une décision qu'elle estimerait illégale et donner un avis sur la délibération modifiée à la suite de cette demande. Si les personnes concernées ne sont pas privées d'un recours juridictionnel contre les délibérations du Comité de sécurité de l'information, elles sont en

revanche privées de la garantie de voir celles-ci soumises au contrôle parlementaire. En effet, ni la nomination et la décharge des membres du Comité de sécurité de l'information par la Chambre des représentants, ni l'obligation de publication annuelle du rapport sommaire de l'accomplissement des missions du Comité de sécurité de l'information sur le site internet de la Banque-carrefour et sur le site internet de la Plate-forme eHealth ne s'apparentent à un tel contrôle.

B.31. Comme la section de législation du Conseil d'État l'a observé dans son avis sur l'avant-projet de loi devenu la loi du 2 avril 2021, pareille délégation à un organisme tel que 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 ce que « les garanties [...] 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 (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, p. 53). Pareilles délégations ne pourraient se justifier que dans la mesure où elles seraient très limitées, en raison de leur portée secondaire ou principalement technique, ce qui n'est pas le cas en l'espèce. Les dispositions, mesures et conditions que les États membres peuvent adopter en vertu de l'article 6, paragraphe 2, de l'article 9, paragraphe 2, point i), et de l'article 9, paragraphe 4, du RGPD ne changent rien à ce constat.

En habilitant la chambre « sécurité sociale et santé » du Comité de sécurité de l'information, dont le statut n'est pas précisé par la loi ni le pouvoir d'appréciation délimité par celle-ci, à prendre des décisions en matière de traitement des données à caractère personnel qui lient les tiers, sans que de telles décisions puissent être soumises au contrôle parlementaire, l'article 5 de l'accord de coopération du 12 mars 2021 prive les personnes concernées de la garantie d'un tel contrôle, sans que cela soit justifié par une exigence découlant du droit de l'Union européenne.

B.32. En ce qu'il est dirigé contre les actes attaqués en ce qu'ils portent assentiment à l'article 5 de l'accord de coopération du 12 mars 2021, le moyen unique, dans sa première branche est fondé dans la mesure où cet article concerne la communication des données visées dans l'article 3, § 2, de l'accord de coopération précité, enregistrées dans la banque de données « Vaccinnet ».

Les actes attaqués doivent être annulés dans cette mesure en ce qu'ils portent assentiment à l'article 5 de l'accord de coopération du 12 mars 2021.

III. En ce qui concerne la durée de conservation des données enregistrées dans « Vaccinnet », visée à l'article 6, § 2 (deuxième branche)

B.33. Dans la deuxième branche du moyen, la partie requérante estime que la durée de conservation des données enregistrées dans « Vaccinnet », prévue par l'article 6, § 2, de l'accord de coopération du 12 mars 2021, est disproportionnée, d'une part, en ce que le délai de 30 ans pour la conservation des données à dater de la date de vaccination contre la COVID-19 serait excessif, et, d'autre part, en l'absence d'un délai maximum de conservation des données.

B.34.1. L'article 6, § 2, de l'accord de coopération du 12 mars 2021 dispose :

« Les données visées à l'article 3, § 2, sont conservées jusqu'au décès de la personne à laquelle le vaccin contre la COVID-19 a été administré et pendant 30 ans au minimum à compter de la vaccination ».

B.34.2. Concernant la durée de conservation des données, visée à l'article 6, l'exposé général de l'accord de coopération du 12 mars 2021 indique :

« Les données relatives au code de vaccination sont conservées jusqu'à 5 jours à compter du lendemain de la publication de l'arrêté royal annonçant la fin de l'épidémie due au coronavirus COVID-19. Un suivi minutieux doit être assuré dans ce cadre aussi longtemps que dure la pandémie.

En outre, l'article 6 régit la durée de conservation des données à caractère personnel de Vaccinnet jusqu'au décès de la personne à laquelle le vaccin contre la COVID-19 a été administré et pendant 30 ans au minimum à compter de la vaccination.

Outre l'importance pour l'utilisateur de soins et les prestataires de soins d'avoir à tout moment une idée précise des vaccinations administrées, ce délai de conservation est requis pour un suivi correct des rappels nécessaires, surtout pour les vaccins pour lesquels la durée de protection n'est pas encore connue. En général, les données à caractère personnel relatives à la santé sont conservées de manière standard dans le dossier médical pendant au moins 30 ans après le dernier contact. La durée de conservation permet par ailleurs un suivi longitudinal à des fins de recherche scientifique. Enfin, ce délai de conservation est important dans le cadre des règles de responsabilité vis-à-vis des acteurs concernés, étant donné l'incertitude relative aux potentiels effets indésirables sur le long terme.

L'intention est qu'un vaccin fonctionne à vie. C'est pourquoi de nombreux vaccins sont administrés à un jeune âge et aucun nouveau vaccin de rappel n'est nécessaire par la suite pour diverses maladies contre lesquelles la vaccination est pratiquée. Il est donc important de savoir si quelqu'un a reçu un certain vaccin même après, par exemple, 30 ans. Il est important pour le médecin mais aussi pour la personne vaccinée de connaître le statut vaccinal des vaccins qui ont été placés il y a longtemps.

En revanche, dans le suivi scientifique de l'efficacité des vaccins, il est également nécessaire de vérifier encore plus qu'après 30 ans si quelqu'un a été vacciné. Par exemple, on a vu que le vaccin contre la coqueluche chez les personnes âgées perd de sa force, de sorte qu'un vaccin de rappel est placé. Pour réaliser ces études, il faut bien sûr savoir s'il y a eu vaccination.

Au plus tard, les effets secondaires des médicaments auxquels appartiennent les vaccins n'apparaissent parfois qu'après de nombreuses années. Un exemple classique de médicament est le diéthylstilbestrol (DES), une hormone administrée aux femmes. On a constaté que de nombreuses filles nées de mères DES avaient un risque accru de cancer du vagin et du col de l'utérus à l'âge adulte. S'ils avaient détruit ces données, ils n'auraient peut-être pas pu établir le lien. Mais les effets différés peuvent également être positifs. Par exemple, il y a l'hypothèse que les personnes (par exemple les enfants) qui ont reçu il y a encore longtemps un vaccin BCG contre la tuberculose pourraient être moins sensibles au COVID-19.

Enfin, un ensemble limité de données en lien avec les résultats de laboratoire provenant de la Base de données I de l'Accord de coopération du 25 août 2020 ne peut pas être supprimé après 60 jours. Ces données sont, en effet, nécessaires pour les processus opérationnels et les finalités liés aux enregistrements des vaccinations. A cet égard, il s'agit dans un premier temps de la finalité de pharmacovigilance. Pour cette finalité, dans le cadre des cas dits ' de percée ' ou ' break through cases ', il pourra être demandé au laboratoire concerné, pour une personne vaccinée qui développe malgré tout la COVID-19, d'effectuer un séquençage du génome complet afin d'analyser la cause de l'échec des vaccinations. Par ailleurs, la conservation de ces données pendant une période plus longue est aussi nécessaire pour la finalité de l'organisation logistique des vaccinations contre la COVID-19. Les données relatives aux contaminations antérieures qui ont permis d'acquérir une certaine immunité, peuvent, en effet, être pertinentes lorsqu'il y a lieu de déterminer la priorité de vaccination des groupes cibles » (*Moniteur belge* du 12 avril 2021, pp. 32411-32412; voy. aussi *Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, pp. 16-18).

B.35.1. Dans son avis sur l'avant-projet de loi devenue la loi du 2 avril 2021 portant assentiment à l'accord de coopération du 12 mars 2021, la section de législation du Conseil d'État a observé :

« 30. Conformément au texte néerlandais de l'article 6, § 2, de l'accord de coopération, les données de la base de données Vaccinet 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 ' » (*ibid.*, pp. 54-55; voy. aussi *Doc. parl.*, Parlement flamand, 2020-2021, n° 708/1, p. 90; *Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, pp. 85-86; *Doc. parl.*, Parlement de la Communauté germanophone, 2020-2021, n° 132/1, pp. 32-33; *Doc. parl.*, Assemblée réunie de la Commission communautaire commune, 2020-2021, n° B-65/1, pp. 18-19; *Doc. parl.*, Assemblée de la Commission communautaire française, 2020-2021, n° 45/1, pp. 33-34).

B.35.2. Dans son avis n° 16/2021 du 10 février 2021 sur l'avant-projet d'accord de coopération devenu l'accord de coopération du 12 mars 2021, l'Autorité de protection des données a observé :

« 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. Sur la durée de conservation des données, la ministre wallonne de la Santé a rappelé que « la durée de validité du vaccin n'est pas encore connue à ce jour » et qu'« il est important de connaître le statut vaccinal d'une personne, en ce compris de nombreuses années après la vaccination » (*Doc. parl.*, Parlement wallon, C.R.I., n° 25, 2020-2021, 31 mars 2021, p. 74).

B.35.4. Devant l'assemblée de la Commission communautaire française, le ministre de la Santé a également précisé :

« 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 » (*Doc. parl.*, Assemblée de la Commission communautaire française, 2020-2021, n° 45/2, p. 12).

B.36.1. Conformément au principe de limitation de la conservation des données, les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (article 5, paragraphe 1, point e), du RGPD).

B.36.2. L'article 6, § 2, de l'accord de coopération du 12 mars 2021 fixe une durée maximale de conservation des données.

Les données enregistrées dans la banque de données « Vaccinnet » sont conservées au minimum 30 ans et au maximum jusqu'à la date du décès de la personne concernée.

B.37.1. La nécessité de la durée de conservation des données s'apprécie au regard des circonstances d'espèce, et en tenant compte du fait que le délai généralement accepté pour la conservation des dossiers concernant la santé et dans le cadre de la recherche scientifique en matière de santé est assez long.

B.37.2. En vertu de l'article 9, § 1er, de la loi du 22 août 2002 sur les droits du patient, le patient « a droit, de la part de son praticien professionnel, à un dossier de patient soigneusement tenu à jour et conservé en lieu sûr » et, à sa demande, « le praticien professionnel ajoute les documents fournis par le patient dans le dossier le concernant ».

Les travaux préparatoires de cette disposition indiquent :

« 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 » (*Doc. parl.*, Chambre, 2001-2002, DOC 50-1642/001, p. 29).

L'article 1er de l'arrêté royal du 3 mai 1999 « relatif au dossier médical général » définit le « dossier médical général » (DMG) comme « un ensemble fonctionnel et sélectif de données médicales, sociales et administratives pertinentes relatives à un patient, qui font l'objet d'un traitement manuel ou informatisé », et qui comprend, notamment « l'anamnèse et les antécédents (maladies, interventions, vaccins reçus) ».

L'article 1er, § 3, de l'arrêté royal du 3 mai 1999 « déterminant les conditions générales minimales auxquelles le dossier médical, visé à l'article 15 de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre », prévoit que le dossier médical ouvert pour chaque patient au sein d'un hôpital « doit être conservé pendant au moins trente ans dans l'hôpital ».

L'article 35 de la loi du 22 avril 2019 « relative à la qualité de la pratique des soins de santé » dispose :

« 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 ».

L'article 24 du Code de déontologie médicale dispose :

« 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 ».

Il résulte de ce qui précède qu'un délai de conservation de 30 ans au moins constitue le délai habituellement accepté en matière de données concernant la santé.

B.37.3. Il convient également d'avoir égard aux circonstances d'urgence pandémique entourant l'élaboration, l'autorisation de mise sur le marché, la production et l'administration des vaccins contre la COVID-19 et la nécessité de pouvoir évaluer, à moyen et à long terme, l'efficacité de ces vaccins, de même que leurs éventuels effets indésirables. C'est notamment dans le but de cette évaluation que les finalités liées à la prestation de soins et de traitement (article 4, § 2, 1°), à la pharmacovigilance des vaccins (article 4, § 2, 2°), au suivi et à la surveillance post-autorisation des vaccins (article 4, § 2, 8°), ou à l'exécution d'études scientifiques ou statistiques (article 4, § 2, 10°) ont été définies.

B.37.4. Au vu de ce qui précède, la conservation des données de vaccination contre la COVID-19 jusqu'au décès de la personne vaccinée n'excède pas ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

B.38. En ce qu'il est dirigé contre les actes attaqués en ce qu'ils portent assentiment à l'article 6, § 2, de l'accord de coopération, le moyen unique, dans sa deuxième branche, n'est pas fondé.

IV. En ce qui concerne l'absence d'analyse d'impact préalable requise par l'article 35 du RGPD (deuxième branche)

B.39. La partie requérante critique l'absence d'exécution d'une analyse d'impact préalable relative à la protection des données, au sens de l'article 35 du RGPD, de sorte qu'en l'absence de cette analyse d'impact, les dispositions visées au moyen seraient violées.

B.40. L'exposé général de l'accord de coopération du 12 mars 2021 indique :

« L'accord de coopération a été soumis à l'avis de l'Autorité de protection des données (avis 16-2021 du 10 février 2021), à l'avis de la ' Vlaamse Toezichtscommissie ' (avis 2021/13 du 17 février 2021), aux avis du Conseil d'Etat (68.832/VR, 68836/VR, 68 837/VR 68.839/VR, 68.840/VR, 68/844/VR du 18 février 2021), à l'avis du Conseil flamand pour l'Aide sociale, la Santé publique et la Famille (avis du 16 février 2021), à l'avis de l'Organe de concertation intra-francophone et de la concertation en Comité ministériel de concertation intra-francophone (avis du 15 février 2021).

Une analyse d'impact relative à la protection des données est établie en application des articles 35 et 36 du Règlement Général sur la Protection des Données » (*Moniteur belge* du 12 avril 2021, p. 32398).

B.41.1. Dans son avis sur l'avant-projet de loi devenue la loi du 2 avril 2021 portant assentiment à l'accord de coopération du 12 mars 2021, la section de législation du Conseil d'État a observé :

« 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 » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, p. 46; voy. aussi *Doc. parl.*, Parlement flamand, 2020-2021, n° 708/1, p. 82; *Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, pp. 81-82; *Doc. parl.*, Parlement de la Communauté germanophone, 2020-2021, n° 132/1, pp. 27-28; *Doc. parl.*, Assemblée réunie de la Commission communautaire commune, 2020-2021, n° B-65/1, pp. 11-12; *Doc. parl.*, Assemblée de la Commission communautaire française, 2020-2021, n° 45/1, p. 29).

B.41.2. Dans son avis n° 16/2021 du 10 février 2021, l'Autorité de protection des données a observé, comme elle l'avait déjà fait dans son avis n° 138/2020 du 18 décembre 2020 relatif à l'arrêté royal du 24 décembre 2020 (point 21) :

« 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 » (point 19).

B.41.3. Dans le rapport du 23 mars 2021, le ministre de la Santé publique a indiqué :

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

B.42. Si le traitement de données personnelles est susceptible d'engendrer un « risque élevé pour les droits et libertés des personnes physiques », le responsable du traitement doit effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel, conformément à l'article 35 du RGPD. En vertu de l'article 36 du RGPD, lorsque l'analyse d'impact indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque, le responsable du traitement doit consulter l'autorité de contrôle préalablement au traitement.

B.43. L'article 35 du RGPD impose la réalisation d'une analyse d'impact relative à la protection des données avant l'acte matériel de traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, mais ne l'impose pas avant ou lors de l'élaboration d'une disposition législative relative à un tel traitement. Dès lors que le caractère préalable de l'analyse d'impact concerne un acte matériel de traitement, il ne relève pas de la compétence de la Cour mais bien de la compétence du juge judiciaire ou administratif.

Ce constat ne porte pas préjudice à l'obligation pour les États membres de consulter « l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement », conformément à l'article 36, paragraphe 4, du RGPD, obligation à laquelle le législateur a déféré en l'espèce.

B.44.1. Enfin, en ce qui concerne la critique dirigée contre la confidentialité de l'analyse d'impact, soulevée par la partie requérante dans son mémoire en réponse, cette critique n'est pas recevable, car elle revient à modifier la portée de la deuxième branche du moyen, qui se limitait à critiquer l'absence d'analyse d'impact préalable.

Il n'appartient en effet pas à une partie requérante de modifier, dans son mémoire en réponse, le moyen tel qu'elle l'a elle-même formulé dans la requête. Un grief qui, comme en l'espèce, est articulé dans un mémoire en réponse mais qui diffère de celui qui est énoncé dans la requête constitue dès lors un moyen nouveau et n'est pas recevable.

B.44.2. Pour le surplus, le RGPD ne fait pas obligation de publier cette analyse (Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, 4 avril 2017, modifiées en dernier lieu le 4 octobre 2017, Groupe de travail « Article 29 » sur la protection des données, p. 21). La confidentialité peut en effet se justifier par le fait que l'analyse d'impact porte sur d'éventuels risques en matière de sécurité, et notamment la description technique des mesures envisagées afin d'atténuer ces risques. Le fait de rendre publique cette analyse risquerait par conséquent de compromettre la sécurité du traitement de ces données, et compromettrait dès lors le droit au respect de la vie privée et de la protection des données personnelles.

B.45. En ce qu'il est dirigé contre les actes attaqués en ce qu'ils n'auraient pas été précédés d'une analyse d'impact préalable, le moyen unique, dans sa deuxième branche, n'est pas fondé.

V. En ce qui concerne la rétroactivité des effets de l'accord de coopération au 24 décembre 2020, prévue par l'article 12 (troisième branche)

B.46. Dans la troisième branche du moyen, la partie requérante estime que les actes attaqués sont contraires au principe de la non-rétroactivité des lois qui 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.

Ainsi, l'article 12 de l'accord de coopération du 12 mars 2021 prévoit que les dispositions de cet accord rétroagissent au jour de l'entrée en vigueur de l'arrêté royal du 24 décembre 2020, alors que, souligne la partie requérante, la onzième finalité reprise dans l'article 4, § 2, de l'accord de coopération ne figurait pas dans l'arrêté royal du 24 décembre 2020.

B.47.1. L'article 12 de l'accord de coopération du 12 mars 2021 dispose :

« Le présent accord de coopération produit ses effets à partir du 24 décembre 2020 pour ce qui concerne les dispositions dont le contenu correspond à celui de l'arrêté royal du 24 décembre 2020 concernant l'enregistrement et le traitement de données relatives aux vaccinations contre la COVID-19 et à partir du 11 février 2021 pour ce qui concerne les autres dispositions.

Le présent accord de coopération produit ses effets jusqu'à sa révision ou sa révocation qui intervient le jour où le Secrétariat central du Comité de concertation a reçu l'accord écrit de toutes les parties pour mettre fin à l'accord de coopération et après la publication d'une communication confirmant cet accord écrit au *Moniteur belge* ».

B.47.2. L'exposé général de l'accord de coopération du 12 mars 2021 indique :

« L'article 12 régit les effets dans le temps de l'accord de coopération et prévoit la possibilité de le réviser ou révoquer » (*Moniteur belge* du 12 avril 2021, p. 32413; voy. aussi *Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, p. 19).

B.48. Dans son avis sur l'avant-projet de loi devenue la loi du 2 avril 2021, attaquée, portant assentiment à l'accord de coopération du 12 mars 2021, la section de législation du Conseil d'État a observé :

« 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 » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, pp. 56-57; voy. aussi *Doc. parl.*, Parlement flamand, 2020-2021, n° 708/1, p. 92; *Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, pp. 86-87; *Doc. parl.*, Parlement de la Communauté germanophone, 2020-2021, n° 132/1, pp. 34-35; *Doc. parl.*, Assemblée réunie de la Commission communautaire commune, 2020-2021, n° B-65/1, pp. 20-21; *Doc. parl.*, Assemblée de la Commission communautaire française, 2020-2021, n° 45/1, p. 35).

B.49.1. Dans le contexte rappelé en B.2, il convient de souligner que l'accord de coopération du 12 mars 2021 a été conclu dans un délai de moins de trois mois, parallèlement au lancement en janvier 2021 de la campagne de vaccination dans des conditions d'urgence, en vue de lutter contre la pandémie de COVID-19.

Par l'arrêté royal du 24 décembre 2020, pris conformément à l'article 11 de la loi du 22 décembre 2020, de même que par le protocole d'accord du 27 janvier 2021, les différentes autorités du pays ont adopté le fondement juridique permettant l'enregistrement des données de vaccination, dans l'attente d'un accord de coopération.

B.49.2. Comme il est dit en B.4, le contenu de l'accord de coopération reprend le contenu du protocole d'accord du 27 janvier 2021 qui, lui-même, reprenait, en l'adaptant, le contenu de l'arrêté royal du 24 décembre 2020. La date d'abrogation de l'arrêté royal du 24 décembre 2020, de même que celle du protocole d'accord du 27 janvier 2021 sont fixées à la date à laquelle l'accord de coopération du 12 mars 2021 sortit ses effets.

Il résulte de ce qui précède que la rétroactivité contenue dans l'article 12 de l'accord de coopération du 12 mars 2021 est justifiée par l'objectif d'intérêt général d'assurer la sécurité juridique en consolidant et remplaçant la base légale de l'enregistrement des données de vaccination dans « Vaccinnet ». Comme l'a souligné la section de législation du Conseil d'État, cette 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 » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, p. 56).

B.49.3. Cette rétroactivité n'entraîne par ailleurs pas d'effets disproportionnés. En prévoyant que l'accord de coopération du 12 mars 2021 produit ses effets à partir du 24 décembre 2020 pour ce qui concerne les dispositions dont le contenu correspond à celui de l'arrêté royal du 24 décembre 2020 « concernant l'enregistrement et le traitement de données relatives aux vaccinations contre la COVID-19 » et à partir du 11 février 2021 pour ce qui concerne les autres dispositions, l'article 12 de l'accord de coopération du 12 mars 2021 ne porte en effet pas atteinte à la sécurité juridique et aux attentes légitimes, dès lors qu'il n'emporte aucune modification du contenu du régime existant antérieurement, mais se limite à le consolider.

Il convient en effet de constater que, pour les éléments qui correspondent au traitement de données à caractère personnel tel qu'il était prévu par l'arrêté royal du 24 décembre 2020, l'accord de coopération sortit ses effets à la date d'entrée en vigueur de cet arrêté royal, tandis que, 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, l'accord de coopération sortit ses effets à la date d'entrée en vigueur du protocole d'accord du 27 janvier 2021, soit le 11 février 2021. Il convient à cet égard de constater que la finalité visée à l'article 4, § 2, 11°, de l'accord de coopération du 12 mars 2021, que critique la partie requérante, était déjà contenue dans le protocole d'accord du 27 janvier 2021.

B.50. En ce qu'il est dirigé contre les actes attaqués en ce qu'ils portent assentiment à l'article 12 de l'accord de coopération du 12 mars 2021, le moyen unique, dans sa troisième branche, n'est pas fondé.

En ce qui concerne la demande de maintien des effets

B.51. Les autorités institutionnelles demandent le maintien des effets des actes attaqués en cas d'annulation.

B.52.1. Lorsqu'un recours en annulation, dirigé contre une norme législative, est fondé, la Cour a uniquement, en vertu de l'article 8, alinéa 1er, de la loi spéciale du 6 janvier 1989, le pouvoir d'annuler l'acte attaqué en tout ou en partie.

Lorsqu'elle annule, comme en l'espèce, une norme législative, de manière inconstitutionnelle, la Cour peut, en vertu de l'article 8, alinéa 3, de la loi spéciale, maintenir provisoirement les effets d'une disposition annulée, jusqu'à ce que le législateur ait mis fin à l'inconstitutionnalité constatée, et pour le délai qu'elle détermine.

B.52.2. Il ressort de la jurisprudence de la Cour de justice que les principes de primauté et de plein effet du droit de l'Union européenne s'opposent à un maintien provisoire de mesures nationales qui sont contraires au droit de l'Union directement applicable (CJUE, grande chambre, 8 septembre 2010, C-409/06, *Winner Wetten GmbH*). Eu égard à cette jurisprudence, la Cour constitutionnelle ne peut donc pas donner suite à une demande de maintien des effets d'un acte législatif annulé, en ce qu'il serait ainsi porté atteinte au plein effet du droit de l'Union.

B.52.3. Pour le surplus, il n'y a pas lieu de faire droit à cette demande, compte tenu de la portée limitée de l'annulation prononcée.

Par ces motifs,

la Cour

- annule la loi du 2 avril 2021, le décret de la Communauté flamande du 2 avril 2021, le décret de la Communauté germanophone du 29 mars 2021, l'ordonnance de la Commission communautaire commune du 2 avril 2021, le décret de la Région wallonne du 1er avril 2021 et le décret de la Commission communautaire française du 1er avril 2021 « portant assentiment à l'accord de coopération du 12 mars 2021 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 », en ce qu'ils portent assentiment à l'article 5 de l'accord de coopération du 12 mars 2021, dans la mesure où cet article concerne la communication des données visées à l'article 3, § 2, de l'accord de coopération précité, enregistrées dans la banque de données « Vaccinnet »;

- rejette le recours pour le surplus.

Ainsi rendu en langue française, en langue néerlandaise et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 1er juin 2023.

Le greffier, Le président,

F. Meersschaut P. Nihoul

GRONDWETTELIJK HOF

[C − 2023/42867]

Uittreksel uit arrest nr. 84/2023 van 1 juni 2023

Rolnummer 7648

In zake : het beroep tot vernietiging van de wet van 2 april 2021, van het decreet van de Vlaamse Gemeenschap van 2 april 2021, van het decreet van de Franse Gemeenschap van 25 maart 2021, van het decreet van de Duitstalige Gemeenschap van 29 maart 2021, van de ordonnantie van de Gemeenschappelijke Gemeenschapscommissie van 2 april 2021, van het decreet van het Waalse Gewest van 1 april 2021 en van het decreet van de Franse Gemeenschapscommissie van 1 april 2021 « houdende instemming met het samenwerkingsakkoord van 12 maart 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waals Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 », ingesteld door Charlotte D'Hondt.

Het Grondwettelijk Hof,

samengesteld uit de voorzitters P. Nihoul en L. Lavrysen, en de rechters T. Giet, J. Moerman, M. Pâques, Y. Kherbache, T. Detienne, D. Pieters, S. de Bethune, E. Bribosia, W. Verrijdt en K. Jadin, bijgestaan door de griffier F. Meersschaut, onder voorzitterschap van voorzitter P. Nihoul,

wijst na beraad het volgende arrest :

I. *Onderwerp van het beroep en rechtspleging*

Bij verzoekschrift dat aan het Hof is toegezonden bij op 7 oktober 2021 ter post aangetekende brief en ter griffie is ingekomen op 8 oktober 2021, heeft Charlotte D'Hondt, bijgestaan en vertegenwoordigd door Mr. P. Joassart, advocaat bij de balie te Brussel, beroep tot vernietiging ingesteld van de wet van 2 april 2021, van het decreet van de Vlaamse Gemeenschap van 2 april 2021, van het decreet van de Franse Gemeenschap van 25 maart 2021, van het decreet van de Duitstalige Gemeenschap van 29 maart 2021, van de ordonnantie van de Gemeenschappelijke Gemeenschapscommissie van 2 april 2021, van het decreet van het Waalse Gewest van 1 april 2021 en van het decreet van de Franse Gemeenschapscommissie van 1 april 2021 « houdende instemming met het samenwerkingsakkoord van 12 maart 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 » (bekendgemaakt respectievelijk in het *Belgisch Staatsblad* van 12 april 2021, tweede editie, van 9 april 2021, van 6 april 2021, van 12 april 2021, tweede editie, van 9 april 2021, van 12 april 2021, tweede editie, en van 7 april 2021).

(...)

II. *In rechte*

(...)

Ten aanzien van de bestreden akten en de context ervan

B.1. De verzoekende partij vordert de vernietiging van de wet van 2 april 2021, van het decreet van de Vlaamse Gemeenschap van 2 april 2021, van het decreet van de Franse Gemeenschap van 25 maart 2021, van het decreet van de Duitstalige Gemeenschap van 29 maart 2021, van de ordonnantie van de Gemeenschappelijke Gemeenschapscommissie van 2 april 2021, van het decreet van het Waalse Gewest van 1 april 2021 en van het decreet van de Franse Gemeenschapscommissie van 1 april 2021 « houdende instemming met het samenwerkingsakkoord van 12 maart 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 » (hierna : het samenwerkingsakkoord van 12 maart 2021).

Het samenwerkingsakkoord van 12 maart 2021 werd, in de drie landstalen, als bijlage bij de wet van 2 april 2021, bekendgemaakt in het *Belgisch Staatsblad* van 12 april 2021.

B.2.1. Op 11 maart 2020 heeft de Wereldgezondheidsorganisatie de uitbraak van het coronavirus SARS-CoV-2 uitgeroepen tot een pandemie. Ook België is sedert maart 2020 geconfronteerd met die pandemie en de gevolgen ervan. Het coronavirus SARS-CoV-2 is een zeer besmettelijk virus dat de ziekte COVID-19 veroorzaakt, die voornamelijk voor ouderen en personen met een medische voorgeschiedenis ernstige medische problemen veroorzaakt of dodelijk kan zijn (*Parl. St.*, Vlaams Parlement, 2019-2020, nr. 415/1, p. 2; *Parl. St.*, Vlaams Parlement, 2020-2021, nr. 488/1, p. 2; *Parl. St.*, Verenigde Vergadering van de Gemeenschappelijke Gemeenschapscommissie, 2019-2020, nr. B-41/1, p. 1).

In het kader van die COVID-19-gezondheidscrisis en om een verdere verspreiding van de ziekte COVID-19 tegen te gaan, werd oorspronkelijk de Nationale Veiligheidsraad en daarna het Overlegcomité, waarin vertegenwoordigers van de federale overheid en van de deelstaten werden opgenomen, belast om op elkaar afgestemde maatregelen te nemen teneinde de verdere verspreiding van COVID-19 te beperken (*Parl. St.*, Vlaams Parlement, 2019-2020, nr. 415/1, p. 2; *Parl. St.*, Vlaams Parlement, 2020-2021, nr. 488/1, p. 2).

B.2.2. De bestreden akten passen in het kader van het aanvullen en het actualiseren van het arsenaal aan maatregelen die de verschillende overheden hebben genomen om de COVID-19-pandemie te bestrijden en de verdere verspreiding van het coronavirus SARS-CoV-2 tegen te gaan, alsook een heropflakkering van de COVID-19-pandemie te vermijden. De bestreden akten passen meer bepaald in het kader van de maatregelen die noodzakelijk zijn voor het organiseren van de vaccinatie tegen COVID-19.

Zoals in andere landen die deelnemen aan de Europese procedure voor de aankoop van vaccins tegen COVID-19, waarin de Europese Commissie namens de lidstaten onderhandelt met de bedrijven, na het verlenen van de vergunning voor het in de handel brengen en naargelang van de productiecapaciteiten, hebben de federale overheid en de deelentiteiten beslist om samen te werken teneinde een massale, vrijwillige en kosteloze vaccinatiecampagne tegen COVID-19 te organiseren.

Die beslissing is met name gebaseerd op studies waaruit de klinische doeltreffendheid blijkt van vaccinatie op grote schaal tegen het zeer besmettelijke coronavirus SARS-CoV-2 dat de ziekte COVID-19 veroorzaakt, teneinde de verspreiding van besmettingen met die ziekte tegen te gaan en te voorkomen dat wegens de daaruit voortvloeiende ziekenhuisopnames worden overbelast, alsook te vermijden dat de COVID-19-pandemie heropflakkert. De Wereldgezondheidsorganisatie raadt het publiek eveneens aan zich te laten vaccineren tegen COVID-19.

De Interministeriële Conferentie Volksgezondheid van 16 november 2020 heeft de hoofdbeginselen vastgesteld waarop de Belgische vaccinatiestrategie tegen COVID-19 is gebaseerd :

- doel van een vaccinatiegraad van 70 % van de bevolking;
- bepalen van de prioritaire groepen op grond van wetenschappelijke adviezen;
- kosteloze vaccinatie op vrijwillige basis voor elke burger;
- medefinanciering van het gehele vaccinatieprogramma door de federale overheid en de deelentiteiten.

Die beslissingen hangen van de volgende elementen af :

- massale vaccinatiecampagnes, waarbij de vaccins worden geleverd in flacons met meerdere doses die dezelfde dag moeten worden toegediend;
- de terbeschikkingstelling aan België van een of meer doeltreffende en veilige vaccins tegen COVID-19;
- de capaciteit van het Belgische gezondheidssysteem voor de geleidelijke en doeltreffende verdeling en vaccinatie van de bevolking, waarbij de autoriteiten voor volksgezondheid worden ondersteund door de Interfederale Taskforce « vaccin COVID-19 », die op 16 november 2020 is opgericht door de Interministeriële Conferentie Volksgezondheid, en de gezamenlijke gezondheidsstructuren van het land, waaronder Sciensano en het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten (FAGG). Daartoe wordt de registratiesoftware Vaccinnet+ door alle deelentiteiten gebruikt;
- de wil om door overtuigingskracht en transparantie de terughoudendheid tegenover het vaccin te overwinnen en zo ervoor te zorgen dat de bevolking die strategie inzake volksgezondheid onderschrijft.

De vaccinatiestrategie tegen COVID-19 werd uitgerold in verschillende fases, vanaf de maand januari 2021, met een hiërarchische indeling van de doelgroepen, waarbij de prioritaire groepen de bewoners van woonzorgcentra en een deel van de personeelsleden van de woonzorgcentra, het ziekenhuispersoneel en het zorg- en hulpverleningspersoneel in de eerste lijn zijn. Vanaf februari 2021 werden de prioritaire groepen uitgebreid tot de risicopersonen met comorbiditeiten, tot de personen die 65 jaar en ouder zijn en tot de personen die 18 tot 55 jaar zijn in de politiediensten, alvorens geleidelijk te worden uitgebreid, op basis van het criterium van de leeftijd en van de kwetsbaarheid, tot de gehele bevolking ouder dan 18 jaar, vervolgens ouder dan 16 jaar, ouder dan 12 jaar en, ten slotte, vanaf 5 jaar.

Op grond van de geactualiseerde wetenschappelijke kennis werd door de Interfederale Taskforce « vaccin COVID-19 » een vaccinatieschema opgesteld met een of twee vaccindoses, naargelang van het toegediende vaccin, en werd de mogelijkheid om een « boosterdosis » te genieten eveneens aan de bevolking aangeboden.

B.2.3.1. Die massale vaccinatiecampagne is ook nauw verbonden met de nieuwe maatregelen die in juli 2020 zijn genomen teneinde de risico's van verdere verspreiding tegen te gaan die zijn verbonden aan de versoepelingen van de beperkingen van fysieke contacten en aan de mogelijkheid om opnieuw te reizen, rekening houdend met de nieuwe fase in de COVID-19-crisis.

B.2.3.2. De verordening (EU) 2021/953 van het Europees Parlement en de Raad van 14 juni 2021 « betreffende een kader voor de afgifte, verificatie en aanvaarding van interoperabele COVID-19-vaccinatie-, test- en herstelcertificaten (digitaal EU-COVID-certificaat) teneinde het vrije verkeer tijdens de COVID-19-pandemie te faciliteren » (hierna : de verordening (EU) 2021/953) voorziet, luidens artikel 1, lid 1, ervan in een kader voor de afgifte, verificatie en aanvaarding van het digitaal EU-COVID-certificaat, zijnde een interoperabel certificaat met informatie over de vaccinatie, het testresultaat of het herstel van de houder ervan, afgegeven in de context van de COVID-19-pandemie, en zulks teneinde de uitoefening van het recht van vrij verkeer door de houders van dergelijke certificaten tijdens de COVID-19-pandemie te faciliteren.

Het digitaal EU-COVID-certificaat maakt de grensoverschrijdende afgifte, verificatie en aanvaarding mogelijk van met name een vaccinatiecertificaat met de bevestiging dat aan de houder ervan een COVID-19-vaccin is toegediend in de lidstaat die het certificaat afgeeft.

In de overwegingen 8 en 29 van de verordening (EU) 2021/953 wordt vermeld :

« 8. Veel lidstaten hebben initiatieven genomen om COVID-19-vaccinatiecertificaten af te geven of zijn voornemens dat te doen. Om dergelijke vaccinatiecertificaten echter doeltreffend te kunnen gebruiken in een grensoverschrijdende context, wanneer Unieburgers hun recht van vrij verkeer uitoefenen, moeten zij volledig interoperabel, compatibel, beveiligd en verifieerbaar zijn. De lidstaten moeten daartoe tot overeenstemming komen over de inhoud, het formaat, de beginselen, de technische normen en het beveiligingsniveau voor dergelijke vaccinatiecertificaten.

[...]

29. Om het vrije verkeer te faciliteren en ervoor te zorgen dat de beperkingen van het vrije verkeer die momenteel tijdens de COVID-19-pandemie van kracht zijn, op gecoördineerde wijze kunnen worden opgeheven op basis van het meest recente wetenschappelijk bewijsmateriaal en de meest recente adviezen van het Gezondheidsbeveiligingscomité, opgericht bij artikel 17 van Besluit nr. 1082/2013/EU van het Europees Parlement en de Raad, het ECDC en het Europees Geneesmiddelenbureau (EMA), moet in een interoperabel vaccinatiecertificaat worden voorzien. Een dergelijk vaccinatiecertificaat moet dienen als bevestiging dat aan de houder een COVID-19-vaccin is toegediend in een lidstaat en moet ertoe bijdragen dat beperkingen van het vrije verkeer geleidelijk worden opgeheven. Het vaccinatiecertificaat mag alleen de informatie bevatten die nodig is om de houder, het toegediende COVID-19-vaccin, het aantal doses, en de datum en de plaats van vaccinatie duidelijk te identificeren. De lidstaten moeten vaccinatiecertificaten afgeven aan personen die zijn ingeënt met COVID-19-vaccins waarvoor op grond van Verordening (EG) nr. 726/2004 van het Europees Parlement en de Raad een vergunning voor het in de handel brengen is verleend, aan personen die zijn ingeënt met COVID-19-vaccins waarvoor op grond van Richtlijn 2001/83/EG van het Europees Parlement en de Raad een vergunning door de bevoegde autoriteit van een lidstaat voor het in de handel brengen is verleend, en aan personen die zijn ingeënt met COVID-19-vaccins waarvan de distributie tijdelijk is toegestaan op grond van artikel 5, lid 2, van die richtlijn ».

Artikel 5 van de verordening (EU) 2021/953, met als opschrift « Vaccinatiecertificaat », bepaalt :

« 1. Elke lidstaat geeft aan personen aan wie een COVID-19-vaccin is toegediend, een in artikel 3, lid 1, punt a), bedoeld vaccinatiecertificaat af, hetzij automatisch, hetzij op verzoek van die personen. Die personen worden in kennis gesteld van hun recht op een vaccinatiecertificaat.

2. Het vaccinatiecertificaat bevat de volgende categorieën persoonsgegevens :

”a”) de identiteit van de houder;

”b”) informatie over het aan de houder toegediende COVID-19-vaccin en over het aantal toegediende doses;

”c”) metagegevens van het certificaat, zoals de afgever van het certificaat of een unieke certificaatidentificatiecode.

De persoonsgegevens worden in het vaccinatiecertificaat opgenomen overeenkomstig de in punt 1 van de bijlage vastgestelde specifieke gegevensvelden.

De Commissie is bevoegd overeenkomstig artikel 12 gedelegeerde handelingen vast te stellen om punt 1 van de bijlage te wijzigen door middel van wijziging of verwijdering van gegevensvelden, of door middel van toevoeging van gegevensvelden die vallen onder de in de punten b) en c) van de eerste alinea van dit lid bedoelde categorieën persoonsgegevens, indien een dergelijke wijziging noodzakelijk is om de echtheid, geldigheid en integriteit van het vaccinatiecertificaat te verifiëren en te bevestigen, in geval van wetenschappelijke vorderingen inzake de beheersing van de COVID-19-pandemie, of om de interoperabiliteit met internationale normen te waarborgen.

3. Het vaccinatiecertificaat wordt na de toediening van elke dosis afgegeven in een beveiligd en interoperabel formaat in overeenstemming met artikel 3, lid 2, en vermeldt duidelijk of de vaccinatiecyclus al dan niet voltooid is.

4. Wanneer nieuw wetenschappelijk bewijs of de interoperabiliteit met internationale normen en technologische systemen zulks om dwingende redenen van urgentie vereist, is de procedure van artikel 13 van toepassing op grond van [de krachtens] dit artikel vastgestelde gedelegeerde handelingen.

5. Lidstaten die een vaccinatiebewijs aanvaarden om vrijstelling te verlenen van overeenkomstig het Unierecht ingestelde beperkingen van het vrije verkeer om de verspreiding van SARS-CoV-2 in te dijken, aanvaarden onder dezelfde voorwaarden ook vaccinatiecertificaten die door andere lidstaten overeenkomstig deze verordening zijn afgegeven voor een COVID-19-vaccin waarvoor op grond van Verordening (EG) nr. 726/2004 een vergunning voor het in de handel brengen is verleend.

De lidstaten kunnen voor hetzelfde doel ook vaccinatiecertificaten aanvaarden die door andere lidstaten overeenkomstig deze verordening zijn afgegeven voor een COVID-19-vaccin waarvoor de bevoegde autoriteit van een lidstaat op grond van Richtlijn 2001/83/EG een vergunning voor het in de handel brengen heeft verleend, een COVID-19-vaccin waarvan de distributie tijdelijk is toegestaan op grond van artikel 5, lid 2, van die richtlijn, of een COVID-19-vaccin waarvoor de WHO-procedure voor noodtoelating is afgerond.

Als lidstaten vaccinatiecertificaten aanvaarden voor een in de tweede alinea bedoeld COVID-19-vaccin, aanvaarden zij onder dezelfde voorwaarden ook vaccinatiecertificaten die door andere lidstaten overeenkomstig deze verordening zijn afgegeven voor hetzelfde COVID-19-vaccin ».

De bijlage, met als opschrift « Datasets voor de certificaten », bepaalt in punt 1 ervan :

« In het vaccinatiecertificaat op te nemen gegevensvelden :

a) naam : familienaam of familienamen en voornaam of voornamen (in die volgorde);

b) geboortedatum;

c) doelziekte of -ziekteverwekker : COVID-19 (SARS-CoV-2 of een van de varianten ervan);

d) COVID-19-vaccin of -profylaxe;

e) productnaam van het COVID-19-vaccin;

f) handelsvergunninghouder of producent van het COVID-19-vaccin;

g) volgnummer in een reeks doses alsook totale aantal doses in de reeks;

h) datum van vaccinatie, met vermelding van de datum van de laatste ontvangen dosis;

i) lidstaat of derde land waar het vaccin werd toegediend;

j) afgever van het certificaat;

k) unieke certificaatidentificatiecode ».

B.2.3.3. In de algemene toelichting bij het samenwerkingsakkoord van 11 juni 2021 tussen de federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de operationalisering van de Verordening (EU) van het Europees Parlement en de Raad betreffende een kader voor de afgifte, verificatie en aanvaarding van interoperabele vaccinatie-, test- en herstelcertificaten teneinde het vrije verkeer tijdens de COVID-19-pandemie te vergemakkelijken (EU Digitaal COVID Certificaat) wordt vermeld :

« Het samenwerkingsakkoord van 12 maart 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 [...] regelt het gemeenschappelijke informatiesysteem dat is opgezet voor de uitnodiging van personen voor vaccinatie, voor de organisatie van de vaccinatie en voor de registratie van de vaccinatie. Door de gefedereerde entiteiten en de federale overheid werd de instelling van een gemeenschappelijk informatiesysteem hiertoe als een cruciale vereiste geformuleerd. Voor de ondersteuning van de uitnodiging van personen voor vaccinatie en de organisatie van de vaccinatie was immers een gemeenschappelijk informatiesysteem nodig om te vermijden dat personen ongecoördineerd worden uitgenodigd of dat reeds gevaccineerde personen opnieuw worden uitgenodigd. Daarnaast maakt het systeem het mogelijk om het geschikt doseringsschema te bepalen, onder meer wat de verschillende doses van een toe te dienen vaccin betreft (juiste interval in geval van vaccin met meerdere dosissen) en ervoor [te] zorgen dat de vaccinatie goed georganiseerd verloopt in functie van de beschikbaarheid van het daartoe benodigde materiaal en (medisch) personeel. De registratie van vaccinaties in een gemeenschappelijk informatiesysteem (Vaccinnet) door zowel Vlaamse, Brusselse, Waalse als Duitstalige vaccinatoren, was dan ook noodzakelijk. [Dergelijke registratieverplichting vergt, gelet op het feit dat het om een noodzakelijkheid gaat en gelet op het feit dat het de verwerking van persoonsgegevens betreft, een solide juridische basis.] Die databank wordt in heel nauwe samenwerking tussen de gefedereerde entiteiten en de Federale Staat uitgewerkt en beheerd. Daarom is het ook aangewezen om ook voor de uitreiking van de certificaten aan de hand van eenzelfde operationeel systeem te werken » (*Belgisch Staatsblad* van 14 juni 2021, tweede editie, p. 61955).

B.2.3.4. De samenwerkingsakkoorden van 14 juli 2021 en van 27 september 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVID-certificaat, het COVID Safe Ticket, het PLF en de verwerking van persoonsgegevens van in het buitenland wonende of verblijvende werknemers en zelfstandigen die activiteiten uitvoeren in België, alsook het samenwerkingsakkoord van 28 oktober 2021, waarbij dat van 14 juli 2021 werd gewijzigd, voorzien in een wettelijke basis voor het binnenlandse gebruik van het digitaal EU-COVID-certificaat en voor het genereren van het COVID Safe Ticket (hierna : het CST) op basis van het digitale EU-COVID-certificaat. De vaccincatie van een persoon tegen het coronavirus COVID-19, kan het CST zonder meer genereren.

In de algemene toelichting bij het voormelde samenwerkingsakkoord van 14 juli 2021 wordt in dat verband vermeld dat, volgens de wetenschappelijke kennis die beschikbaar was op het ogenblik dat het akkoord werd aangenomen, personen die gevaccineerd zijn een kleiner risico lopen om andere personen te besmetten met het coronavirus SARS-CoV-2 (*Belgisch Staatsblad* van 23 juli 2021, p.76172; zie ook overweging 7 van de verordening (EU) 2021/953).

Artikel 11 van het samenwerkingsakkoord van 14 juli 2021 bepaalt :

« § 1. Met het oog op de verificatie en voor het opmaken en afgeven van het digitaal EU-COVID-certificaat aan de houders van een vaccinatiecertificaat, testcertificaat of herstelcertificaat, worden de volgende categorieën van persoonsgegevens verwerkt :

1° de categorieën van persoonsgegevens in artikel 9, §§ 1, 2 of 3;

2° het identificatienummer bedoeld in artikel 8 van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid; en

3° de hoofdverblijfplaats, bedoeld in artikel 3, eerste lid, 5°, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen.

§ 2. De categorieën van persoonsgegevens vermeld in § 1 worden bekomen vanuit de volgende gegevensbanken :

[...]

2° Vaccinnet : voor wat betreft het identificatienummer bedoeld in artikel 8 van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid en de categorieën van persoonsgegevens in het vaccinatiecertificaat, omschreven in artikel 9, § 1;

[...]

§ 4. In afwijking van artikel 3, § 1, van het samenwerkingsakkoord van 25 augustus 2020 en artikel 4, § 2, van het samenwerkingsakkoord van 12 maart 2021, mogen de persoonsgegevens bedoeld in § 1, voor het in artikel 10 bedoelde verwerkingsdoeleinde worden verwerkt door de verwerkingsverantwoordelijken, voor de uitoefening van hun wettelijke opdrachten in dit samenwerkingsakkoord bepaald, de gefedereerde entiteiten en Sciensano ».

B.3.1. Bij het samenwerkingsakkoord van 12 maart 2021 hebben de federale overheid en de gefedereerde entiteiten « het gemeenschappelijke informatiesysteem [...] voor de uitnodiging van personen voor vaccinatie, voor de organisatie van de vaccinatie en voor de registratie van de vaccinatie » opgezet (*Belgisch Staatsblad* van 12 april 2021, tweede editie, p. 32397) :

« De registratie van vaccinaties in een gemeenschappelijk informatiesysteem (Vaccinnet) door zowel Vlaamse, Brusselse, Waalse als Duitstalige vaccinatoren, is o.a. noodzakelijk om een optimaal crisisbeheer te voeren, de geneesmiddelenbewaking, zoals bedoeld in artikel 4, 2° van dit akkoord, mogelijk te maken, de vaccinatiegraad van de bevolking en de impact op de ziekteverzekering op te volgen.

Dergelijke registratieverplichting vergt, gelet op het feit dat het om een noodzakelijkheid gaat en gelet op het feit dat het de verwerking van persoonsgegevens betreft[,] een solide juridische basis.

De databank wordt in heel nauwe samenwerking tussen de gefedereerde entiteiten en de Federale Staat uitgewerkt en beheerd » (*ibid.*, pp. 32397-32398).

B.3.2. In die context regelt het samenwerkingsakkoord van 12 maart 2021 twee verschillende gegevensbanken.

Enerzijds wordt een eerste gegevensbank met de vaccinatiecodes opgericht « om de massale vaccinatiecampagne in het kader van de COVID-19-pandemie in goede banen te leiden door het volgende mogelijk te maken, namelijk de uitnodiging van de te vaccineren personen, de identificatie van het juiste doseringsschema en de goede organisatie van de vaccinatie naargelang de beschikbaarheid van de vaccins en het materiaal en het hiervoor noodzakelijk (medisch en verpleegkundig) personeel » (*ibid.*, p. 32398).

Die gegevensbank genereert een willekeurige vaccinatiecode voor de gehele bevolking die *a priori* kan worden gevaccineerd, en verzamelt de gegevens betreffende die personen om het vaccinatieschema tegen COVID-19 te coördineren en te vermijden dat een nieuwe vaccinatiecode wordt gegenereerd voor een persoon die reeds is gevaccineerd (artikel 2, § 1). De in die gegevensbank geregistreerde gegevens worden vastgesteld bij artikel 3, § 1, van het samenwerkingsakkoord van 12 maart 2021. Zij worden bewaard tot vijf dagen na de dag van publicatie van het koninklijk besluit dat het einde van de toestand van de coronavirus SARS-CoV-2 afkondigt (artikel 6, § 1).

Anderzijds heeft een tweede gegevensbank, « Vaccinnet », betrekking op de registratie voor het gehele land, door de persoon die het vaccin tegen COVID-19 heeft toegediend of zijn gevolmachtigde, van de vaccinatiegegevens als dusdanig van de personen die zich hebben laten vaccineren (artikel 2, § 2). De vaccinatiegegevens worden in artikel 3, § 2, van het samenwerkingsakkoord van 12 maart 2021 omschreven als de identiteitsgegevens betreffende de persoon aan wie het vaccin wordt toegediend (1°), de identiteits- en eventueel contactgegevens betreffende de persoon die het vaccin heeft toegediend (2°), de gegevens betreffende het vaccin (3°), de datum en de plaats van toediening van elke dosis van het vaccin (4°), de gegevens over het schema voor vaccinatie tegen COVID-19 van de persoon aan wie het vaccin wordt toegediend (5°) en, in voorkomend geval, de gegevens over de ongewenste bijwerkingen vastgesteld tijdens of na de vaccinatie van de betrokken persoon, waarvan de persoon die het vaccin heeft toegediend of diens gevolmachtigde kennis heeft (6°). Die gegevens worden bewaard tot aan het overlijden van de persoon aan wie het vaccin tegen COVID-19 werd toegediend en minimum gedurende 30 jaar na de vaccinatie (artikel 6, § 2).

De gegevensbank « Vaccinnet » « beoogt verschillende doelstellingen in verband met de vaccinatie. Het betreft de kwaliteitsvolle zorgverlening, de geneesmiddelenbewaking, de traceerbaarheid van de vaccins, het beheer van de vaccinatieschema's, de logistieke organisatie van de vaccinatie, de bepaling van de vaccinatiegraad, de organisatie van de contactopvolging, de uitvoering van de opvolging en van het toezicht, de berekening van de verdeling van de vaccinatiekosten, het verrichten van wetenschappelijk of statistisch onderzoek » (*ibid.*, p. 32400).

De verwerkingsdoeleinden van de in de twee gegevensbanken geregistreerde gegevens worden vermeld in artikel 4 van het samenwerkingsakkoord van 12 maart 2021. De in die twee gegevensbanken opgenomen gegevens « mogen niet aan derden worden overgemaakt behalve wanneer een wet, een decreet of een ordonnantie een derde machtigt om toegang te hebben tot dergelijke gegevens of die te krijgen zodat ze enkel dezelfde doeleinden met betrekking tot de vaccinatie kunnen beogen als die bedoeld in artikel 4 van het samenwerkingsakkoord » (*ibid.*, p. 32401), na machtiging door het Informatieveiligheidscomité.

Voor de twee gegevensbanken treden de bevoegde deelentiteiten of de door de bevoegde deelentiteiten aangeduide agentschappen en de federale overheid, ieder in het kader van hun bevoegdheid, op als verwerkingsverantwoordelijke voor de verwerking van de gegevens (artikel 7, § 1). Voor de personen voor wie de federale overheid bevoegd is, wordt Sciensano geïdentificeerd als de verwerkingsverantwoordelijke voor de verwerking van de gegevens (artikel 7, § 1, 7°). Er wordt in een centraal contactpunt per entiteit en in een elektronisch toegangsrecht voorzien (artikel 7, § 2).

De Interministeriële Conferentie Volksgezondheid houdt toezicht op de uitvoering en op de naleving van het samenwerkingsakkoord van 12 maart 2021 (artikel 9, § 1).

B.4.1. De bepalingen van het samenwerkingsakkoord van 12 maart 2021 komen in hoofdzaak overeen met die van het koninklijk besluit van 24 december 2020 « betreffende de registratie en de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 » (hierna : het koninklijk besluit van 24 december 2020), waartegen de verzoekende partij ook een beroep tot nietigverklaring heeft ingesteld bij de Raad van State. In de aanhef van dat koninklijk besluit werd vermeld dat « het van vitaal belang is voor de volksgezondheid en voor het vermijden van een heropflakkering van de COVID-19-pandemie, dat de nodige maatregelen inzake de vaccinaties kunnen worden genomen » (*Belgisch Staatsblad* van 24 december 2020, tweede editie, p. 94404) , in afwachting van het sluiten van een samenwerkingsakkoord.

Dat koninklijk besluit is in werking getreden op 24 december 2020, datum van de bekendmaking ervan in het *Belgisch Staatsblad*.

Artikel 9 van het koninklijk besluit van 24 december 2020 bepaalde :

« Dit besluit treedt in werking op de dag van zijn publicatie in het *Belgisch Staatsblad* en houdt op uitwerking te hebben op de dag waarop een Samenwerkingsakkoord tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de registratie en de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 in werking treedt ».

B.4.2.1. Het koninklijk besluit van 24 december 2020 werd genomen overeenkomstig artikel 11 van de wet van 22 december 2020 « houdende diverse maatregelen met betrekking tot snelle antigeentesten en de registratie en verwerking van gegevens betreffende vaccinaties in het kader van de strijd tegen de COVID-19-pandemie » (hierna : de wet van 22 december 2020), dat bepaalde :

« De arts of verpleegkundige die een vaccin tegen COVID-19 toedient of onder wiens toezicht de vaccinatie gebeurt, registreert elke vaccinatie in de databank die door de Interministeriële Conferentie Volksgezondheid wordt aangeduid. De Koning bepaalt, bij een besluit overlegd in de Ministerraad, de nadere modaliteiten van deze registratie en omschrijft minstens de doeleinden van de gegevensverwerking, de categorieën van personen waarover gegevens worden verwerkt, de categorieën gegevens die worden verwerkt, de verantwoordelijken voor de gegevensverwerking en de bewaartermijn van de gegevens ».

B.4.2.2. In de parlementaire voorbereiding van de wet van 22 december 2020 wordt in dat verband uiteengezet :

« Artikel 11 legt de verplichting op om iedere vaccinatie tegen COVID-19 te registreren. Enkel artsen of verpleegkundigen zijn wettelijk bevoegd om vaccinaties toe te dienen. De vaccinatie en de registratie kan wel gebeuren door andere personen onder hun toezicht.

De registratie van vaccinaties is noodzakelijk om een onderbouwd crisisbeheer te voeren, de medische opvolging (vigilantie) van de gevaccineerde te garanderen, de immuniteitsopbouw van de bevolking op te volgen en de impact op de ziekteverzekering en het aantal te verwachten hospitalisaties in te schatten.

De registratie van een vaccinatie impliceert de opname in een gegevensbank van gegevens over de gevaccineerde persoon, gegevens over de persoon die het vaccin toedient, gegevens over het vaccin, gegevens over de omstandigheden van het toedienen van het vaccin en gegevens over eventuele ongewenste bijwerkingen van het vaccin.

De databank zal in heel nauwe samenwerking met de deelstaten worden aangelegd en beheerd. Daartoe zal de Interministeriële Conferentie Volksgezondheid de databank aanduiden waarbinnen bedoelde gegevens worden opgeslagen.

Aan de Koning wordt de bevoegdheid gegeven om nadere regelen en voorwaarden te bepalen, met bijzondere aandacht voor de aspecten die de bescherming van de privacy betreffen.

Het spreekt echter voor zich dat de persoonsgegevens die verzameld en verwerkt worden in het kader van deze registratie, worden verwerkt overeenkomstig de regelgeving over de bescherming bij de verwerking van persoonsgegevens, in het bijzonder de Algemene Verordening Gegevensbescherming, de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform.

De gefedereerde entiteiten en de federale overheid hebben het voornemen om de registratie en de gegevensverwerking die ze inhoudt nader te regelen in een Samenwerkingsakkoord in de zin van artikel 92*bis* van de bijzondere wet van 8 augustus 1980 tot hervorming van de instellingen. Gelet op de hoogdringendheid van het opstarten van de vaccinatie en de absolute noodzaak tot registratie van de vaccinaties voor de hogervermelde redenen, wordt inmiddels voorzien in voorliggende regelgeving » (*Parl. St.*, Kamer, 2020-2021, DOC 55-1677/001, pp. 10-11).

B.4.2.3. Artikel 11 van de wet van 22 december 2020 werd opgeheven bij artikel 11 van het samenwerkingsakkoord van 12 maart 2021.

B.4.3. In de aanhef van het koninklijk besluit van 24 december 2020 wordt vermeld dat de vaccinatiegegevensbank werd aangeduid door de Interministeriële Conferentie Volksgezondheid van 3 december 2020 (*Belgisch Staatsblad* van 24 december 2020, p. 94404). In artikel 1, 2°, van het koninklijk besluit van 24 december 2020 wordt de « vaccinatiegegevensbank » gedefinieerd als « de gegevensbank aangeduid door de Interministeriële Conferentie Volksgezondheid in uitvoering van artikel 11 van de wet van 22 december 2020 houdende diverse maatregelen met betrekking tot snelle antigeentesten en de registratie en verwerking van gegevens betreffende vaccinaties in het kader van de strijd tegen de COVID-19-pandemie ».

De parlementaire voorbereiding van de wet van 22 december 2020 vermeldt over die gegevensbank :

« Het wetsvoorstel voorziet in een dringende wettelijke grondslag voor de verplichting tot registratie en de verzameling van gegevens met betrekking tot de vaccinatie. Deze registratie is noodzakelijk om alle aspecten van het crisisbeheer te kunnen opvolgen. Er werd voor geopteerd om alle registraties van de verschillende vaccinaties te registreren op de Vlaamse vaccinatiedatabank VaccinNet » (*Parl. St.*, Kamer, 2020-2021, DOC 55-1677/002, p. 4).

B.4.4.1. Een protocolakkoord van 27 januari 2021 « tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 » (hierna : het protocolakkoord van 27 januari 2021) neemt de inhoud van de bepalingen van het koninklijk besluit van 24 december 2020 grotendeels over. In de aanhef van dat protocolakkoord wordt vermeld dat dat protocol « tot stand is gekomen met respect voor de bevoegdheidsverdeling die krachtens de bijzondere wet tot hervorming der instellingen aan de verschillende bevoegdheidsniveaus [werd] toegekend dankzij een intense samenwerking in de schoot van de Interministeriële Conferentie die kadert in een lange traditie van samenwerking binnen de Interministeriële Conferentie Volksgezondheid tussen de verschillende bevoegdheidsniveaus van ons land » en dat, « in het kader van de vaccinatie COVID-19, een registratie van de vaccinatiegegevens in een gemeenschappelijke databank, door zowel Vlaamse, Brusselse, Waalse als Duitstalige vaccinatoren, absoluut noodzakelijk is voor verschillende doeleinden » (*Belgisch Staatsblad* van 11 februari 2021, p. 13033).

In artikel 1, 3°, van het protocolakkoord van 27 januari 2021 wordt « Vaccinnet » gedefinieerd als « het registratiesysteem bedoeld in artikel 9 van het besluit van de Vlaamse Regering van 16 mei 2014 houdende diverse bepalingen ter uitvoering van het [Vlaamse] decreet van 21 november 2003 betreffende het preventieve gezondheidsbeleid en tot wijziging van uitvoeringsbesluiten van dit decreet ». Overeenkomstig artikel 43 van het voormelde decreet van 21 november 2003 moeten de vaccinatoren meewerken aan het registratiesysteem « Vaccinnet » wanneer de Vlaamse Regering, op grond van haar bevoegdheid inzake preventief gezondheidsbeleid, een vaccinatieschema opstelt dat de voor de bevolking aanbevolen vaccinaties weergeeft.

De in het protocolakkoord van 27 januari 2021 bedoelde gegevensbank « Vaccinnet » vormt aldus een uitbreiding, wat de vaccinaties tegen COVID-19 betreft, van de bestaande gegevensbank « Vaccinnet » die op het niveau van de Vlaamse Gemeenschap is opgericht. De verdeling van de kosten voor de ontwikkeling van « Vaccinnet » werd vastgesteld in artikel 6 van het protocolakkoord van 9 februari 2022 tussen de federale Regering en de in de artikelen 128, 130 en 135 van de Grondwet bedoelde overheden « inzake de cofinanciering van het COVID-19[-]vaccinatieprogramma ».

B.4.4.2. Artikel 11 van het protocolakkoord van 27 januari 2021 bepaalt :

« Onderhavig protocolakkoord is geen samenwerkingsakkoord zoals bedoeld in artikel 92*bis* van de bijzondere wet van 8 augustus 1980 tot hervorming van de instellingen. Partijen streven ernaar om, op basis van de bepalingen van dit protocolakkoord, een samenwerkingsakkoord te bereiken tegen 21 april 2021 ».

Artikel 12 van het protocolakkoord van 27 januari 2021 bepaalt :

« Dit protocolakkoord heeft uitwerking met ingang van 24 december 2020 en houdt op uitwerking te hebben op de dag waarop een Samenwerkingsakkoord tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 in werking treedt ».

B.5. Overeenkomstig artikel 12, eerste lid, ervan heeft het samenwerkingsakkoord van 12 maart 2021 uitwerking met ingang van 24 december 2020 voor wat betreft de bepalingen die inhoudelijk overeenstemmen met het koninklijk besluit van 24 december 2020 betreffende de registratie en de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 en met ingang van 11 februari 2021 voor wat betreft de andere bepalingen.

Overeenkomstig artikel 9 van het koninklijk besluit van 24 december 2020 en artikel 12 van het protocolakkoord van 27 januari 2021 hebben het koninklijk besluit van 24 december 2020 en het protocolakkoord van 27 januari 2021 opgehouden uitwerking te hebben op de dag van de inwerkingtreding van het samenwerkingsakkoord van 12 maart 2021, zijnde op 22 april 2021.

B.6. De zeven bestreden wetgevingen (hierna : de bestreden akten) beperken zich ertoe instemming te verlenen met het samenwerkingsakkoord van 12 maart 2021.

Ten aanzien van de ontvankelijkheid ratione temporis *van het beroep*

B.7. De Waalse Regering, de Vlaamse Regering, de Franse Gemeenschapsregering, de Regering van de Duitstalige Gemeenschap, het College van de Franse Gemeenschapscommissie en het Verenigd College van de Gemeenschappelijke Gemeenschapscommissie zijn van mening dat het beroep tot vernietiging, dat op 7 oktober 2021 is ingesteld, klaarblijkelijk niet ontvankelijk is *ratione temporis* in zoverre het is gericht tegen het instemmingsdecreet van de Franse Gemeenschap van 25 maart 2021, dat is bekendgemaakt in het *Belgisch Staatsblad* op 6 april 2021.

B.8.1. Om te voldoen aan de vereisten van artikel 3, § 1, van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof moet een beroep tot vernietiging worden ingesteld binnen een termijn van zes maanden na de bekendmaking van de bestreden norm in het *Belgisch Staatsblad*.

B.8.2. De voormelde bepaling maakt met betrekking tot de aanvang van de termijn om een beroep tot vernietiging in te stellen tegen de bestreden norm geen onderscheid, naargelang daarbij al dan niet instemming wordt verleend met een samenwerkingsakkoord.

In tegenstelling tot hetgeen de verzoekende partij aanvoert, neemt de termijn om een beroep tot vernietiging in te stellen tegen akten waarbij instemming wordt verleend met een samenwerkingsakkoord, geen aanvang vanaf de inwerkingtreding van dat samenwerkingsakkoord, maar begint die te lopen vanaf de datum van de bekendmaking van de bestreden akten.

B.8.3. Het Hof heeft reeds in een reeks voorafgaande arresten te kennen gegeven dat - bij ontstentenis van een nadere precisering in de bijzondere wet van 6 januari 1989 en naar analogie met de regeling van artikel 54 van het Gerechtelijk Wetboek - voor het bepalen van de termijn voor het instellen van een beroep of van een vordering tot schorsing moet worden gerekend van de zoveelste tot de dag vóór de zoveelste (zie arrest nr. 125/2012 van 18 oktober 2012, ECLI:BE:GHCC:2012:ARR.125, B.2; nr. 169/2016 van 22 december 2016, ECLI:BE:GHCC:2016:ARR.169, B.2).

Het instemmingsdecreet van de Franse Gemeenschap van 25 maart 2021 werd bekengemaakt in het *Belgisch Staatsblad* van 6 april 2021. De termijn om een beroep in te stellen tegen die akte heeft dus een aanvang genomen op 7 april 2021 en is verstreken op 6 oktober 2021. Daaruit volgt dat het beroep tot vernietiging dat is ingesteld bij een op 7 oktober 2021 ter post afgegeven verzoekschrift, klaarblijkelijk niet ontvankelijk is.

B.8.4. In zoverre het is gericht tegen het instemmingsdecreet van de Franse Gemeenschap van 25 maart 2021, is het beroep tot vernietiging, niet ontvankelijk *ratione temporis*.

Ten aanzien van de omvang van het beroep tot vernietiging

B.9.1. Om te voldoen aan de vereisten van artikel 6 van de bijzondere wet van 6 januari 1989, moeten de middelen van het verzoekschrift te kennen geven welke van de regels waarvan het Hof de naleving waarborgt, zouden zijn geschonden, alsook welke de bepalingen zijn die deze regels zouden schenden, en uiteenzetten in welk opzicht die regels door de bedoelde bepalingen zouden zijn geschonden.

B.9.2. Het Hof bepaalt de omvang van het beroep tot vernietiging aan de hand van de inhoud van het verzoekschrift en in het bijzonder op basis van de uiteenzetting van de middelen. Het Hof beperkt zijn onderzoek tot de bepalingen waartegen daadwerkelijk grieven zijn aangewend.

B.10.1. Uit de uiteenzetting van het enige middel blijkt dat de grieven van de verzoekende partij enkel tegen de bestreden akten zijn gericht in zoverre daarbij instemming wordt verleend met een aantal bepalingen van het samenwerkingsakkoord van 12 maart 2021 die de registratie en de verwerking van persoonsgegevens in de gegevensbank « Vaccinnet » regelen, die de verzoekende partij in haar middel uitdrukkelijk identificeert :

- artikel 2, § 2, dat betrekking heeft op de registratie van de vaccinatiegegevens;
- artikel 3, § 2, dat de in « Vaccinnet » verzamelde vaccinatiegegevens bepaalt;
- artikel 4, § 2, dat de doeleinden voor de verwerking van de in artikel 3, § 2, bedoelde gegevens vaststelt;
- artikel 5, dat het mogelijk maakt om in « Vaccinnet » vermelde gegevens mee te delen aan derden;
- artikel 6, § 2, dat de bewaringstermijn van de in artikel 3, § 2, bedoelde gegevens vaststelt;
- artikel 12, dat de datum van inwerkingtreding van de bepalingen van het samenwerkingsakkoord van 12 maart 2021 vaststelt.

B.10.2. Wanneer de verzoekende partij die bepalingen in haar enige middel bekritiseert, formuleert zij evenwel geen enkele grief tegen het beginsel zelf van de registratie van de vaccinatiegegevens, noch tegen de in « Vaccinnet » verzamelde vaccinatiegegevens. Buiten een algemene kritiek zet zij niet uiteen in welk opzicht de bestreden akten, door instemming te verlenen met de artikelen 2, § 2, en 3, § 2, van het samenwerkingsakkoord van 12 maart 2021, de in het middel bedoelde bepalingen zouden schenden.

In zoverre in het enige middel die bepalingen worden beoogd, beantwoordt het bijgevolg niet aan de vereisten van artikel 6 van de bijzondere wet van 6 januari 1989.

B.10.3. Het Hof beperkt bijgevolg zijn onderzoek van het beroep tot vernietiging dat is gericht tegen de bestreden akten in zoverre daarbij instemming wordt verleend met de artikelen 4, § 2, 5 en 6, § 2, van het samenwerkingsakkoord van 12 maart 2021 en met artikel 12 van het voormelde samenwerkingsakkoord, in zoverre dat laatste artikel de datum van inwerkingtreding van de voormelde artikelen 4, § 2, 5 en 6, § 2, vaststelt.

Het beroep tot vernietiging is bijgevolg niet ontvankelijk doordat het is gericht tegen de bestreden akten in zoverre daarbij instemming wordt verleend met de andere bepalingen van het voormelde samenwerkingsakkoord.

B.10.4. Het Hof brengt in herinnering dat het de bestreden akten niet op zinvolle wijze kan toetsen zonder de inhoud van de relevante bepalingen van het voormelde samenwerkingsakkoord in zijn onderzoek te betrekken.

Ten aanzien van het belang van de verzoekende partij

B.11. De verzoekende partij verantwoordt haar belang om in rechte te treden door het feit dat zij een natuurlijke persoon is die in België verblijft en in aanmerking komt voor vaccinatie tegen COVID-19, zodat de bestreden akten haar rechtstreeks en ongunstig kunnen raken. Indien zij beslist om zich te laten vaccineren, zullen haar naam en haar verschillende persoonsgegevens immers worden vermeld in « Vaccinnet », met schending van haar recht op eerbiediging van het privéleven, in samenhang gelezen met het beginsel van de niet-retroactiviteit van de wetten. Indien zij daarentegen beslist om zich niet te laten vaccineren, zou er een ernstig risico bestaan dat er beperkingen zijn waardoor zij wordt geraakt om reden van haar niet-vaccinatie.

B.12. De Ministerraad, de Waalse Regering, de Vlaamse Regering, de Franse Gemeenschapsregering, de Regering van de Duitstalige Gemeenschap, het College van de Franse Gemeenschapscommissie en het Verenigd College van de Gemeenschappelijke Gemeenschapscommissie betwisten het belang van de verzoekende partij om in rechte te treden, aangezien zij menen dat haar vordering veel weg heeft van een *actio popularis*.

B.13. De Grondwet en de bijzondere wet van 6 januari 1989 vereisen dat elke natuurlijke persoon of rechtspersoon die een beroep tot vernietiging instelt, doet blijken van een belang. Van het vereiste belang doen slechts blijken de personen wier situatie door de bestreden norm rechtstreeks en ongunstig zou kunnen worden geraakt.

B.14.1. Krachtens het niet-bestreden artikel 2, § 1, van het samenwerkingsakkoord van 12 maart 2021 dient iedere natuurlijke persoon die zich op het grondgebied van België bevindt, door middel van een COVID-19-vaccinatiecode een uitnodiging te krijgen om zich te laten vaccineren, overeenkomstig de door de bevoegde overheden vastgestelde vaccinatiestrategie. Die betekenisloze vaccinatiecode wordt gegenereerd door de gegevensbank die overeenkomstig het niet-bestreden artikel 3, § 1, van het samenwerkingsakkoord van 12 maart 2021 wordt geregeld.

Overeenkomstig artikel 2, § 2, van het samenwerkingsakkoord van 12 maart 2021 geeft elke vaccinatie aanleiding tot de registratie, in « Vaccinnet », van de in artikel 3, § 2, van het samenwerkingsakkoord van 12 maart 2021 vermelde vaccinatiegegevens. Alle personen die zich tegen COVID-19 laten vaccineren, worden bijgevolg onderworpen aan de automatische registratie van hun vaccinatiegegevens in de gegevensbank « Vaccinnet » en aan de verwerking van die gegevens in overeenstemming met wat in dat samenwerkingsakkoord is vermeld.

Als natuurlijke persoon die zich op het grondgebied van België bevindt, werd de verzoekende partij noodzakelijkerwijs uitgenodigd om zich te laten vaccineren en kon zij de uitnodiging om zich te laten vaccineren enkel aanvaarden door ermee in te stemmen dat haar vaccinatiegegevens worden geregistreerd en verwerkt in « Vaccinnet » overeenkomstig de bestreden akten waarbij instemming wordt verleend met het samenwerkingsakkoord van 12 maart 2021. De gevolgen van de bestreden akten inzake de verwerking van de vaccinatiegegevens kunnen bijgevolg de keuze van de verzoekende partij met betrekking tot haar vaccinatie tegen COVID-19 rechtstreeks beïnvloeden

B.14.2. Uit het voorgaande vloeit voort dat de bestreden akten de verzoekende partij rechtstreeks en ongunstig kunnen raken in haar beslissing om zich te laten vaccineren.

B.14.3. Voor het overige beperkt het samenwerkingsakkoord van 12 maart 2021 zich tot het regelen van het gemeenschappelijk systeem voor de registratie van de COVID-19-vaccinatiegegevens op het grondgebied van België. Dat samenwerkingsakkoord roept geen vaccinatieplicht in het leven, aangezien de in B.2.2 uiteengezette vaccinatiestrategie is gebaseerd op een vrijwillige en kosteloze vaccinatie.

In tegenstelling tot hetgeen de verzoekende partij aanvoert, voorzien de bestreden akten niet in enig gevolg dat verband zou houden met het gebrek aan vaccinatie. De gevolgen van een vaccinatiecertificaat, maar ook van een test- en herstelcertificaat, voor het verkrijgen van een CST, worden bepaald in de samenwerkingsakkoorden van 14 juli 2021, 27 september 2021 en 28 oktober 2021, die zijn aangehaald in B.2.3.4. Niet alleen toont de verzoekende partij niet aan dat de beperkingen waarop zij zich beroept en die uit het gebrek aan vaccinatie zouden voortvloeien, echt zijn - hetgeen volstaat om vast te stellen dat het aangevoerde nadeel louter hypothetisch is -, maar die eventuele beperkingen vormen evenmin een nadeel dat rechtstreeks zou voortvloeien uit de akten die bij het onderhavige beroep worden bestreden.

In zoverre zij zich beroept op de gevolgen in verband met de niet-vaccinatie tegen COVID-19, doet de verzoekende partij niet blijken van het vereiste belang.

Ten gronde

B.15. Het enige middel is afgeleid uit de schending van artikel 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, met de artikelen 5, 6, 9 en 35 van de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 « betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) » (hierna : de AVG), en met het beginsel van de niet-retroactiviteit van de wetten.

B.16.1. Artikel 22 van de Grondwet bepaalt :

« Ieder heeft recht op eerbiediging van zijn privé-leven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald.

De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht ».

B.16.2. Artikel 8 van het Europees Verdrag voor de rechten van de mens bepaalt :

« 1. Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn gezinsleven, zijn huis en zijn briefwisseling.

2. Geen inmenging van enig openbaar gezag is toegestaan met betrekking tot de uitoefening van dit recht dan voor zover bij de wet is voorzien en in een democratische samenleving nodig is in het belang van 's lands veiligheid, de openbare veiligheid, of het economisch welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden, of voor de bescherming van de rechten en vrijheden van anderen ».

B.16.3. De Grondwetgever heeft gestreefd naar een zo groot mogelijke concordantie tussen artikel 22 van de Grondwet en artikel 8 van het Europees Verdrag voor de rechten van de mens (*Parl. St.*, Kamer, 1992-1993, nr. 997/5, p. 2).

De draagwijdte van dat artikel 8 is analoog aan die van de voormelde grondwetsbepaling, zodat de waarborgen die beide bepalingen bieden, een onlosmakelijk geheel vormen.

B.16.4. Het recht op eerbiediging van het privéleven, zoals gewaarborgd in de voormelde grondwets- en verdragsbepalingen, heeft als essentieel doel de personen te beschermen tegen inmengingen in hun privéleven.

Dat recht heeft een ruime draagwijdte en omvat, onder meer, de eerbiediging van de fysieke integriteit van de persoon (EHRM, grote kamer, 8 april 2021, *Vavřička e.a. t. Tsjechië*, ECLI:CE:ECHR:2021:0408JUD004762113, § 261) en de bescherming van persoonsgegevens en van persoonlijke informatie met betrekking tot de gezondheid (EHRM, 25 februari 1997, *Z. t. Finland*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; 10 oktober 2006, *L.L. t. Frankrijk*, ECLI:CE:ECHR:2006:1010JUD000750802, § 32; 27 februari 2018, *Mockuté t. Litouwen*, ECLI:CE:ECHR:2018:0227JUD006649009, § 93). Uit de rechtspraak van het Europees Hof voor de Rechten van de Mens blijkt dat, onder meer, de volgende gegevens en informatie betreffende personen vallen onder de bescherming van dat recht : de naam, het adres, de professionele activiteiten, de persoonlijke relaties, digitale vingerafdrukken, camerabeelden, foto's, communicatiegegevens, DNA-gegevens, gerechtelijke gegevens (veroordeling of verdenking), financiële gegevens, informatie over bezittingen en medische gegevens (zie onder meer EHRM, 26 maart 1987, *Leander t. Zweden*, ECLI:CE:ECHR:1987:0326JUD000924881, §§ 47-48; grote kamer, 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, ECLI:CE:ECHR:2008:1204JUD003056204, §§ 66-68; 17 december 2009, *B.B. t. Frankrijk*, ECLI:CE:ECHR:2009:1217JUD000533506, § 57; 10 februari 2011, *Dimitrov-Kazakov t. Bulgarije*, ECLI:CE:ECHR:2011:0210JUD001137903, §§ 29-31; 18 oktober 2011, *Khelili t. Zwitserland*, ECLI:CE:ECHR:2011:1018JUD001618807, §§ 55-57; 9 oktober 2012, *Alkaya t. Turkije*, ECLI:CE:ECHR:2012:1009JUD004281106, § 29; 18 april 2013, *M.K. t. Frankrijk*, ECLI:CE:ECHR:2013:0418JUD001952209, § 26; 18 september 2014, *Brunet t. Frankrijk*, ECLI:CE:ECHR:2014:0918JUD002101010, § 31; 13 oktober 2020, *Frâncu t. Roemenië*, ECLI:CE:ECHR:2020:1013JUD006935613, § 51).

De bescherming van persoonsgegevens met betrekking tot de gezondheid is niet alleen van fundamenteel belang voor de eerbiediging van het privéleven van de persoon, maar ook voor zijn of haar vertrouwen in de gezondheidszorg (EHRM, 25 februari 1997, *Z. t. Finland*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95). Zonder die bescherming zouden personen ervan kunnen worden afgehouden om gevoelige en persoonlijke informatie te delen met zorgverstrekkers of met diensten van de gezondheidszorg waardoor ze niet alleen hun eigen gezondheid, maar, in geval van besmettelijke ziekten, ook de samenleving in gevaar kunnen brengen (*ibid.*, § 95).

B.16.5. Het recht op eerbiediging van het privéleven is evenwel niet absoluut. Artikel 22 van de Grondwet en artikel 8 van het Europees Verdrag voor de rechten van de mens sluiten een overheidsinmenging in de uitoefening van dat recht niet uit, voor zover zij wordt toegestaan door een voldoende precieze wettelijke bepaling, zij beantwoordt aan een dwingende maatschappelijke behoefte in een democratische samenleving en zij evenredig is met de daarmee nagestreefde wettige doelstelling. Die bepalingen houden voor de overheid bovendien de positieve verplichting in om maatregelen te nemen die een daadwerkelijke eerbiediging van het privéleven garanderen, zelfs in de sfeer van de onderlinge verhoudingen tussen individuen (EHRM, 27 oktober 1994, *Kroon e.a. t. Nederland*, ECLI:CE:ECHR:1994:1027JUD001853591, § 31; grote kamer, 12 november 2013, *Söderman t. Zweden*, ECLI:CE:ECHR:2013:1112JUD000578608, § 78).

Wanneer zij de afweging maken tussen het belang van de Staat bij de verwerking van persoonsgegevens en het individueel belang bij de bescherming van de vertrouwelijkheid van die gegevens, beschikken de nationale autoriteiten over een zekere beoordelingsmarge (*ibid.*, § 99). Gezien het fundamentele belang van de bescherming van persoonsgegevens is die marge evenwel vrij beperkt (EHRM, 26 januari 2017, *Surikov t. Oekraïne*, ECLI:CE:ECHR:2017:0126JUD004278806, § 73). Opdat een norm verenigbaar is met het recht op eerbiediging van het privéleven, is vereist dat een billijk evenwicht wordt bereikt tussen alle rechten en belangen die in het geding zijn. Bij de beoordeling van dat evenwicht dient rekening te worden gehouden met de bepalingen van het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (hierna : het Verdrag nr. 108) (EHRM, 25 februari 1997, *Z t. Finland*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; grote kamer, 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, ECLI:CE:ECHR:2008:1204JUD003056204 § 103; 26 januari 2017, *Surikov t. Oekraïne*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

Het Verdrag nr. 108 bevat onder meer de beginselen inzake de verwerking van persoonsgegevens : rechtmatigheid, behoorlijkheid, transparantie, doelbinding, evenredigheid, juistheid, opslagbeperking, integriteit en vertrouwelijkheid, en verantwoordingsplicht.

Datzelfde Verdrag is geactualiseerd bij een protocol tot amendering dat op 10 oktober 2018 voor ondertekening is opengesteld.

Uit het Verdrag nr. 108 vloeit voort dat het nationale recht in het bijzonder moet garanderen dat persoonsgegevens relevant en niet excessief zijn in het licht van de doeleinden waarvoor ze worden verzameld of bijgehouden, dat de gegevens worden bewaard in een vorm die de identificatie van de betrokkenen niet langer dan vereist mogelijk maakt, en dat de bijgehouden data op efficiënte wijze worden beschermd tegen verkeerdelijk gebruik en misbruik. Het heeft ook erop gewezen dat het van essentieel belang is dat het nationale recht duidelijke en gedetailleerde regels bevat inzake de reikwijdte en toepassing van de betrokken maatregelen, en ook minimumwaarborgen bevat inzake, onder andere, de duurtijd, de bewaring, het gebruik, de toegang van derden, procedures voor het behoud van de integriteit en vertrouwelijkheid van gegevens en procedures voor de vernietiging ervan, zodat in elke fase van de gegevensverwerking er voldoende waarborgen zijn tegen het risico van misbruik en willekeur (EHRM, 26 januari 2017, *Surikov t. Oekraïne*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

B.16.6. Binnen de werkingssfeer van het Europees Unierecht waarborgen artikel 22 van de Grondwet, artikel 8 van het Europees Verdrag voor de rechten van de mens en artikel 7 van het Handvest analoge grondrechten (HvJ, grote kamer, 9 november 2010, C-92/09 en C-93/09, *Volker und Markus Schecke GbR e.a.*, ECLI:EU:C:2010:662), terwijl artikel 8 van dat Handvest een specifieke rechtsbescherming van persoonsgegevens beoogt.

B.16.7. Het Hof van Justitie van de Europese Unie oordeelt dat de eerbiediging van het recht op persoonlijke levenssfeer bij de verwerking van persoonsgegevens gelijk welke informatie betreft aangaande een geïdentificeerde of identificeerbare natuurlijke persoon (HvJ, grote kamer, 9 november 2010, C-92/09 en C-93/09, *Volker und Markus Schecke GbR e.a.*, ECLI:EU:C:2010:662, punt 52; 16 januari 2019, C-496/17, *Deutsche Post AG*, ECLI:EU:C:2019:26, punt 54).

B.16.8. De in de artikelen 7 en 8 van het Handvest verankerde grondrechten hebben evenmin een absolute gelding (HvJ, grote kamer, 16 juli 2020, C-311/18, *Data Protection Commissioner*, ECLI:EU:C:2020:559, punt 172).

Overeenkomstig artikel 52, lid 1, eerste volzin, van het Handvest van de grondrechten van de Europese Unie moeten beperkingen op de uitoefening van de daarin erkende rechten en vrijheden, waaronder met name het door artikel 7 gewaarborgde recht op eerbiediging van het privéleven en het in artikel 8 ervan neergelegde recht op bescherming van persoonsgegevens, bij wet worden gesteld, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan een doelstelling van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen (HvJ, grote kamer, 6 oktober 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, punt 64). In diezelfde zin moeten overeenkomstig artikel 23 van de AVG beperkingen van bepaalde daarin opgenomen verplichtingen van de verwerkingsverantwoordelijken en de rechten van de betrokkenen worden ingesteld bij wet, de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laten, in een democratische samenleving een noodzakelijke en evenredige maatregel zijn ter verwezenlijking van het nagestreefde doel, en de in het tweede lid geformuleerde specifieke vereisten naleven (HvJ, grote kamer, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, ECLI:EU:C:2020:791, punten 209-210; 10 december 2020, C-620/19, *Land Nordrhein-Westfalen*, ECLI:EU:C:2020:1011, punt 46).

B.16.9. Bij artikel 22 van de Grondwet wordt aan de bevoegde wetgever de bevoegdheid voorbehouden om te bepalen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven. Het waarborgt aldus aan elke burger dat geen inmenging in de uitoefening van dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering.

Een delegatie aan een andere macht is evenwel niet in strijd met het wettigheidsbeginsel, voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgesteld.

Bijgevolg moeten de essentiële elementen van de verwerking van persoonsgegevens in de wet, het decreet of de ordonnantie zelf worden vastgelegd. In dat verband maken de volgende elementen, ongeacht de aard van de betrokken aangelegenheid, in beginsel essentiële elementen uit : (1°) de categorie van verwerkte gegevens; (2°) de categorie van betrokken personen; (3°) de met de verwerking nagestreefde doelstelling; (4°) de categorie van personen die toegang hebben tot de verwerkte gegevens en (5°) de maximumtermijn voor het bewaren van de gegevens (advies van de algemene vergadering van de afdeling wetgeving van de Raad van State nr. 68.936/AV van 7 april 2021 over een voorontwerp van wet « betreffende de maatregelen van bestuurlijke politie tijdens een epidemische noodsituatie » (*Parl. St.*, Kamer, 2020-2021, DOC 55-1951/001, p. 119).

B.16.10. Naast het formele wettigheidsvereiste legt artikel 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens en met de artikelen 7, 8 en 52 van het Handvest van de grondrechten van de Europese Unie, de verplichting op dat de inmenging in het recht op eerbiediging van het privéleven en in het recht op bescherming van persoonsgegevens in duidelijke en voldoende nauwkeurige bewoordingen wordt geformuleerd die het mogelijk maken de hypothesen te voorzien waarin de wetgever een dergelijke inmenging in het recht op eerbiediging van het privéleven toestaat.

Inzake de bescherming van de persoonsgegevens impliceert dat vereiste van voorzienbaarheid dat voldoende precies moet worden bepaald in welke omstandigheden de verwerkingen van persoonsgegevens zijn toegelaten (EHRM, grote kamer, 4 mei 2000, *Rotaru t. Roemenië*, ECLI:CE:ECHR:2000:0504JUD002834195, § 57; grote kamer, 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, ECLI:CE:ECHR:2008:1204JUD003056204, § 99). Het vereiste dat de beperking bij wet dient te worden ingesteld, houdt met name in dat de rechtsgrond die de inmenging in die rechten toestaat, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht moet bepalen (HvJ, 6 oktober 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, punt 65).

Derhalve moet eenieder een voldoende duidelijk beeld kunnen hebben van de verwerkte gegevens, de bij een bepaalde gegevensverwerking betrokken personen en de voorwaarden voor en de doeleinden van de verwerking.

B.16.11. Artikel 5 van de AVG, met als opschrift « Beginselen inzake verwerking van persoonsgegevens », bepaalt :

« 1. Persoonsgegevens moeten :

″a″) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (‘ rechtmatigheid, behoorlijkheid en transparantie ’);

″b″) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd (‘ doelbinding ’);

″c″) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (‘ minimale gegevensverwerking ’);

″d″) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren (‘ juistheid ’);

″e″) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen (‘ opslagbeperking ’);

″f″) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (‘ integriteit en vertrouwelijkheid ’).

2. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen (‘ verantwoordingsplicht ’) ».

Artikel 6 van de AVG, met als opschrift « Rechtmatigheid van de verwerking », bepaalt :

« 1. De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan :

″a″) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;

″b″) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;

″c″) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

″d″) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;

″e″) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;

″f″) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

De eerste alinea, punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken.

2. De lidstaten kunnen specifiekere bepalingen handhaven of invoeren ter aanpassing van de manier waarop de regels van deze verordening met betrekking tot de verwerking met het oog op de naleving van lid 1, punten c) en e), worden toegepast; hiertoe kunnen zij een nadere omschrijving geven van specifieke voorschriften voor de verwerking en andere maatregelen om een rechtmatige en behoorlijke verwerking te waarborgen, ook voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX.

3. De rechtsgrond voor de in lid 1, punten c) en e), bedoelde verwerking moet worden vastgesteld bij :

″a″) Unierecht; of

″b″) lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is.

Het doel van de verwerking wordt in die rechtsgrond vastgesteld of is met betrekking tot de in lid 1, punt e), bedoelde verwerking noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend. Die rechtsgrond kan specifieke bepalingen bevatten om de toepassing van de regels van deze verordening aan te passen, met inbegrip van de algemene voorwaarden inzake de rechtmatigheid van verwerking door de verwerkingsverantwoordelijke; de types verwerkte gegevens; de betrokkenen; de entiteiten waaraan en de doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; de doelbinding; de opslagperioden; en de verwerkingsactiviteiten en -procedures, waaronder maatregelen om te zorgen voor een rechtmatige en behoorlijke verwerking, zoals die voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX. Het Unierecht of het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel.

4. Wanneer de verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld niet berust op toestemming van de betrokkene of op een Unierechtelijke bepaling of een lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in artikel 23, lid 1, bedoelde doelstellingen houdt de verwerkingsverantwoordelijke bij de beoordeling van de vraag of de verwerking voor een ander doel verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld onder meer rekening met :

″a″) ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenomen verdere verwerking;

″b″) het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft;

″c″) de aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens worden verwerkt, overeenkomstig artikel 9, en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt, overeenkomstig artikel 10;

″d″) de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen;

″e″) het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering ».

Artikel 9 van de AVG, met als opschrift « Verwerking van bijzondere categorieën van persoonsgegevens », bepaalt :

« 1. Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

2. Lid 1 is niet van toepassing wanneer aan een van de onderstaande voorwaarden is voldaan :

″a″) de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven;

[...]

″h″) de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen;

″i″) de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim;

[...]

3. De in lid 1 bedoelde persoonsgegevens mogen worden verwerkt voor de in lid 2, punt h), genoemde doeleinden wanneer die gegevens worden verwerkt door of onder de verantwoordelijkheid van een beroepsbeoefenaar die krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels aan het beroepsgeheim is gebonden, of door een andere persoon die eveneens krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels tot geheimhouding is gehouden.

4. De lidstaten kunnen bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid handhaven of invoeren ».

Artikel 35 van de AVG, met als opschrift « Gegevensbeschermingseffectbeoordeling », bepaalt :

« 1. Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.

2. Wanneer een functionaris voor gegevensbescherming is aangewezen, wint de verwerkingsverantwoordelijke bij het uitvoeren van een gegevensbeschermingseffectbeoordeling diens advies in.

3. Een gegevensbeschermingseffectbeoordeling als bedoeld in lid 1 is met name vereist in de volgende gevallen :

″a″) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;

″b″) grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10; of

″c″) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

4. De toezichthoudende autoriteit stelt een lijst op van het soort verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling overeenkomstig lid 1 verplicht is, en maakt deze openbaar. De toezichthoudende autoriteit deelt die lijsten mee aan het in artikel 68 bedoelde Comité.

5. De toezichthoudende autoriteit kan ook een lijst opstellen en openbaar maken van het soort verwerking waarvoor geen gegevensbeschermingseffectbeoordeling is vereist. De toezichthoudende autoriteit deelt deze lijst mee aan het Comité.

6. Wanneer de in de leden 4 en 5 bedoelde lijsten betrekking hebben op verwerkingen met betrekking tot het aanbieden van goederen of diensten aan betrokkenen of op het observeren van hun gedrag in verschillende lidstaten, of op verwerkingen die het vrije verkeer van persoonsgegevens in de Unie wezenlijk kunnen beïnvloeden, past de bevoegde toezichthoudende autoriteit voorafgaand aan de vaststelling van die lijsten het in artikel 63 bedoelde coherentiemechanisme toe.

7. De beoordeling bevat ten minste :

″a″) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;

″b″) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;

″c″) een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkenen; en

″d″) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

8. Bij het beoordelen van het effect van de door een verwerkingsverantwoordelijke of verwerker verrichte verwerkingen, en met name ter wille van een gegevensbeschermingseffectbeoordeling, wordt de naleving van de in artikel 40 bedoelde goedgekeurde gedragscodes naar behoren in aanmerking genomen.

9. De verwerkingsverantwoordelijke vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van verwerkingen.

10. Wanneer verwerking uit hoofde van artikel 6, lid 1, onder c) of e), haar rechtsgrond heeft in het Unierecht of in het recht van de lidstaat dat op de verwerkingsverantwoordelijke van toepassing is, de specifieke verwerking of geheel van verwerkingen in kwestie daarbij wordt geregeld, en er reeds als onderdeel van een algemene effectbeoordeling in het kader van de vaststelling van deze rechtsgrond een gegevensbeschermingseffectbeoordeling is uitgevoerd, zijn de leden 1 tot en met 7 niet van toepassing, tenzij de lidstaten het noodzakelijk achten om voorafgaand aan de verwerkingen een dergelijke beoordeling uit te voeren.

11. Indien nodig verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden ».

B.16.12. De niet-retroactiviteit van de wetten is een waarborg die tot doel heeft rechtsonzekerheid te voorkomen. Die waarborg vereist dat de inhoud van het recht voorzienbaar en toegankelijk is, zodat de rechtzoekende de gevolgen van een bepaalde handeling in redelijke mate kan voorzien op het ogenblik dat die handeling wordt gesteld. De terugwerkende kracht is enkel verantwoord indien die absoluut noodzakelijk is voor de verwezenlijking van een doelstelling van algemeen belang.

Indien blijkt dat de terugwerkende kracht bovendien tot doel of tot gevolg heeft dat de afloop van gerechtelijke procedures in een welbepaalde zin wordt beïnvloed of dat de rechtscolleges worden verhinderd zich uit te spreken over een welbepaalde rechtsvraag, vereist de aard van het in het geding zijnde beginsel dat uitzonderlijke omstandigheden of dwingende motieven van algemeen belang het optreden van de wetgever verantwoorden, dat, ten nadele van een categorie van burgers, afbreuk doet aan de aan allen geboden jurisdictionele waarborgen.

B.17. De grieven van de verzoekende partij hebben betrekking op de volgende aspecten :

I. de doeleinden van de verwerking van de vaccinatiegegevens, bedoeld in artikel 4, § 2 (eerste onderdeel) (B.18-B.24);

II. de aan het Informatieveiligheidscomité verleende machtiging om de mededeling van persoonsgegevens aan derden toe te staan, bedoeld in artikel 5 (eerste onderdeel) (B.25-B.32);

III. de bewaringstermijn van de in « Vaccinnet » geregistreerde gegevens, bedoeld in artikel 6 (tweede onderdeel) (B.33-B.38);

IV. de ontstentenis van een voorafgaande effectbeoordeling, vereist bij artikel 35 van de AVG (tweede onderdeel) (B.39-B.45);

V. de terugwerkende kracht van de gevolgen van het samenwerkingsakkoord tot 24 december 2020, bedoeld in artikel 12 (derde onderdeel) (B.46-B.50).

I. Wat betreft de doeleinden van de verwerking van de vaccinatiegegevens, bedoeld in artikel 4, § 2 (eerste onderdeel)

B.18. In het eerste onderdeel van het middel is de verzoekende partij van mening dat de elf doeleinden die zijn omschreven in artikel 4, § 2, van het samenwerkingsakkoord van 12 maart 2021, niet voldoende « welbepaald en uitdrukkelijk omschreven » zijn, zodat ten aanzien van essentiële elementen van de verwerking van gevoelige persoonsgegevens de beginselen van wettigheid en van voorzienbaarheid niet in acht worden genomen. Zij bekritiseert meer bepaald het ruime karakter van het in het 1° bedoelde doeleinde en de noodzaak van het in het 11° bedoelde doeleinde.

B.19. Artikel 4, § 2, van het samenwerkingsakkoord van 12 maart 2021 bepaalt :

« De verwerking van de persoonsgegevens bedoeld in artikel 3, § 2, beoogt de volgende verwerkingsdoeleinden :

1° het verstrekken van gezondheidszorg en behandelingen, zoals bedoeld in artikel 9, 2, h van de Algemene Verordening Gegevensbescherming, wat uitsluitend beoogd wordt door de vaccinatie en de ondersteunings-, de informatie- en de sensibiliseringsmaatregelen ten aanzien van de burgers voor wat de vaccinatie betreft;

2° de geneesmiddelenbewaking van de vaccins tegen COVID-19, overeenkomstig artikel 12*sexies* van de wet van 25 maart 1964 op de geneesmiddelen en de gedetailleerde richtsnoeren bekendgemaakt door de Europese Commissie in de ' Module VI - Verzameling, beheer en indiening van meldingen van vermoedelijke bijwerkingen van geneesmiddelen (GVP) ', zoals ze voorkomen in de laatst beschikbare versie, en zoals bedoeld in artikel 4, paragraaf 1, 3e lid, 3°, van de wet van 20 juli 2006 betreffende de oprichting en de werking van het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten;

3° de traceerbaarheid van de vaccins tegen COVID-19 teneinde de opvolging van ' rapid alerts van vigilantie ' en ' rapid alerts van kwaliteit ' te verzekeren zoals bedoeld in artikel 4, paragraaf 1, 3e lid, 3°, e, en 4°, j, van de wet van 20 juli 2006 betreffende de oprichting en de werking van het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten;

4° het beheren van schema's voor vaccinatie tegen COVID-19 per te vaccineren of gevaccineerde persoon en het inplannen van vaccinatiemomenten, onder meer door de vaccinatiecentra;

5° de logistieke organisatie van de vaccinatie tegen COVID-19, na anonimisering van de gegevens of ten minste pseudonimisering van de gegevens voor het geval dat de anonimisering de logistieke organisatie niet mogelijk zou maken;

6° het bepalen van de anonieme vaccinatiegraad tegen COVID-19 van de bevolking;

7° het organiseren van de contactopsporing in uitvoering van het Samenwerkingsakkoord van 25 augustus 2020 tussen de Federale Staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie, betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde gefedereerde entiteiten of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano;

8° het uitvoeren van de monitoring en surveillance na vergunning van de vaccins overeenkomstig de goede praktijken aanbevolen door de Wereldgezondheidsorganisatie, na anonimisering van de gegevens of ten minste pseudonimisering van de gegevens voor het geval dat de anonimisering de monitoring en surveillance na vergunning niet mogelijk zou maken;

9° onverminderd de regelgeving inzake de ziekteverzekering, de berekening van de verdeling van de kosten voor de vaccinatie tussen de Federale Staat en de gefedereerde entiteiten, na anonimisering van de gegevens of ten minste pseudonimisering van de gegevens voor het geval dat de anonimisering de berekening van de verdeling niet mogelijk zou maken;

10° het uitvoeren van wetenschappelijke of statistische studies, in overeenstemming met artikel 89, § 1 van de Algemene Verordening Gegevensbescherming en in voorkomend geval met artikel 89, §§ 2 en 3 van de Algemene Verordening Gegevensbescherming en titel 4 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, na anonimisering, of minstens pseudonimisering, voor het geval dat anonimisering niet zou toelaten de wetenschappelijke of statistische studie uit te voeren;

11° het informeren en sensibiliseren van personen met betrekking tot de COVID-19 vaccinatie door zorgverleners en verzekeringsinstellingen ».

B.20.1. Wat de in artikel 4 bedoelde doeleinden betreft, wordt in de algemene toelichting bij het samenwerkingsakkoord van 12 maart 2021 vermeld :

« Artikel 4 omschrijft per gegevensbank de verwerkingsdoeleinden; het betreft in het algemeen volgende doeleinden :

- een kwalitatieve zorgverstrekking aan de betrokkene wat uitsluitend beoogd wordt door de vaccinatie en de ondersteunings-, informatie- en sensibiliseringsmaatregelen ten aanzien van de burgers voor wat de vaccinatie betreft;

- de geneesmiddelenbewaking;

- de traceerbaarheid van de vaccins;

- het beheren van schema's voor vaccinatie tegen COVID-19 en het inplannen van vaccinatiemomenten, onder meer door de vaccinatiecentra en zorgverleners;

- de logistieke organisatie van de vaccinatie tegen COVID-19; wat dit betreft, is het nuttig erop te wijzen dat om dit doeleinde te bereiken, zowel de vaccinatiecodes-gegevensbank als de gegevensbank voor registratie van de vaccinaties noodzakelijk zijn, waarbij de laatste databank onder meer toelaat om de eerste te voeden, bijvoorbeeld om te vermijden dat reeds gevaccineerde personen opnieuw uitgenodigd worden of om de behoeftes op het vlak van vaccins of medisch personeel te bepalen rekening houdend met de vaccinaties die nog toegediend moeten worden;

- het bepalen van de anonieme vaccinatiegraad tegen COVID-19 van de bevolking;

- het organiseren van de contactopsporing;

- het uitvoeren van de monitoring en surveillance na vergunning van de vaccins;

- de berekening van de verdeling van de kosten voor de vaccinatie tussen de Federale Staat en de gefedereerde entiteiten;

- het ondersteunen van wetenschappelijk onderzoek, onder meer inzake de doeltreffendheid en de veiligheid van de vaccins;

- het informeren en sensibiliseren van personen met betrekking tot de vaccinatie tegen COVID-19 door de gezondheidsinspecties van de gefedereerde entiteiten, de zorgverleners en de verzekeringsinstellingen om een maximale vaccinatiegraad te beogen;

- het uitnodigen, en het aanbieden van ondersteuning bij het uitnodigingsproces, van personen voor vaccinatie tegen COVID-19 door de zorgverleners, de verzekeringsinstellingen, de vaccinatiecentra, de federale overheid, de bevoegde gefedereerde entiteiten en de lokale besturen.

Wat het doeleinde inzake monitoring en surveillance na vergunning van de vaccins betreft, kunnen de volgende elementen worden aangehaald.

Studies over de aanvaarding en het gebruik van de vaccins en de vaccinatiegraad laten toe te achterhalen hoeveel personen bereid zijn om zich te laten vaccineren en hoeveel het ook effectief doen. Meer bepaald laten studies over de vaccinatiegraad toe om het percentage van gevaccineerde personen te ramen binnen specifieke risicogroepen, zoals ouderen of personen met specifieke onderliggende aandoeningen. Deze studies zullen inzicht bieden in de houding van de bevolking ten aanzien van de vaccins en zullen toelaten om lacunes in het vaccinatieprogramma te identificeren.

De opvolging van de doeltreffendheid, de seroprevalentie en de immunogeniciteit van de vaccins laat toe te evalueren in welke mate het vaccin een immuniteitsrespons opwekt en een besmetting voorkomt op lange termijn en in geval van circulatie van nieuwe virusstammen.

Ten slotte is het essentieel om te waken over de kwaliteit van de vaccins en een systeem te implementeren dat toelaat om laattijdige of zeldzame ongewenste nevenwerkingen te detecteren om de veiligheid van de vaccins blijvend te garanderen.

Over het algemeen worden de resultaten van de surveillance na vergunning gebruikt om het vaccinbeleid te sturen en om de zorgverleners en de bevolking in het algemeen te informeren over de resultaten van het COVID-19-vaccinatieprogamma in België.

In elk geval worden deze monitoring en surveillance na vergunning van de vaccins georganiseerd overeenkomstig de goede praktijken die op dat vlak aanbevolen worden door de Wereldgezondheidsorganisatie.

Het belang van de link met contact tracing dient te worden beklemtoond, aangezien één van de doeleinden de organisatie van contact tracing betreft. De beoogde scenario's waarbij de link gelegd wordt tussen de vaccinatie en de contact tracing moeten noodzakelijk kaderen binnen de exclusieve doelstelling van opvolging van besmettelijke contacten en opvolging van de vaccinatie. Hierbij kan onder meer gedacht worden aan volgende scenario's :

- het advies dat door het contactcenter dient te worden gegeven kan verschillen naargelang iemand al dan niet gevaccineerd is;

- de bron is gevaccineerd maar heeft een aantal contacten besmet; dit betreft een geval van vaccin failure of een variant strain waar het vaccin niet tegen beschermt en dus heel belangrijke informatie voor de volksgezondheid;

- de bron is niet gevaccineerd, waardoor anderen besmet geraakt zijn;

- contacten kunnen gevaccineerd zijn, waardoor de epidemie uitdooft aangezien het vaccin een doeltreffende preventiemaatregel blijkt te zijn;

- contacten zijn niet gevaccineerd, waarbij de epidemie verder actief in kaart moet worden gebracht.

De gegevens die in dit kader vanuit Vaccinnet naar de gegevensbank bij Sciensano worden overgedragen betreffen *a priori* het INSZ, de vaccinatiestatus en het type vaccin maar flexibiliteit blijft noodzakelijk op basis van evoluerende wetenschappelijke inzichten inzake de impact van vaccinatie op besmettingsrisico's.

Daarnaast dient beklemtoond te worden dat de persoonsgegevens nodig zijn voor de medische opvolging van de patiënt in relatie met de vaccinatie tegen COVID-19, aangezien een hoge vaccinatiegraad binnen de bevolking een belangrijke en fundamentele uitdaging op het vlak van volksgezondheid vormt ten aanzien van de ongeziene COVID-19-pandemie, terwijl het op het niveau van het individu ook belangrijk is dat de betrokkene een geïnformeerde keuze kan maken voor zijn persoonlijke gezondheid. Dit vergt inderdaad een combinatie van algemene en gerichte informatie (op initiatief van de behandelend arts of de verzekeringsinstelling voor hun eigen patiënten en leden). Het is onder meer van essentieel belang dat de arts (de huisarts, de specialist), op basis van zijn gedetailleerde kennis van de medische voorgeschiedenis van de aan zijn zorgen toevertrouwde patiënt, oordeelt over het al dan niet belangrijk zijn van de vaccinatie van de patiënt, die zelf naar behoren is geïnformeerd. In dit kader moet tevens worden beklemtoond dat permanent gewaakt moet worden over een voldoende vaccinatiegraad (bijvoorbeeld 70 procent) en het van belang is dit gericht (via campagnes en individueel) te kunnen opvolgen. Vanzelfsprekend kunnen personen, die duidelijk te kennen gegeven hebben dat zij het vaccin weigeren, niet ongewenst worden benaderd.

Wat niet beoogd wordt door het doeleinde van kwalitatieve zorgverstrekking is de toegang tot kwalitatieve zorgverstrekking op enige manier beperken of afhankelijk stellen in functie van de vaccinatiestatus van een persoon.

Vervolgens kan worden opgemerkt dat het bepalen van de anonieme vaccinatiegraad tegen COVID-19 fijnmazig moet kunnen gebeuren (bijvoorbeeld in woonzorgcentra moet een onderscheid gemaakt worden tussen zorgpersoneel en residenten) en dit niet steeds kan worden gerealiseerd aan de hand van anonieme of minstens gepseudonimiseerde persoonsgegevens ingeval de anonimisering niet zou toelaten om het beoogde doel te realiseren.

Bovendien moet worden benadrukt dat in principe alle categorieën van gegevens geregistreerd zowel in de vaccinatiecodes-gegevensbank als in de gegevensbank voor registratie van de vaccinaties voor élk doeleinde kunnen worden verwerkt en bewaard. De tekst van het samenwerkingsakkoord verduidelijkt daarnaast waar het enkel anonieme of minstens gepseudonimiseerde gegevens betreft, ingeval de anonimisering niet zou toelaten om het beoogde doel te realiseren.

De gegevens die in het kader van dit samenwerkingsakkoord worden ingezameld, mogen niet voor andere doeleinden dan die voorzien in dit akkoord worden gebruikt.

De krachtens dit samenwerkingsakkoord verzamelde gegevens mogen niet worden gebruikt voor andere dan de in dit artikel bepaalde doelstellingen, in het bijzonder maar niet uitsluitend politionele, commerciële, fiscale, strafrechtelijke of [aan staatsveiligheid verbonden doelstellingen.]

Ten slotte moet het gebruik van de gegevens uit de gegevensbanken vanzelfsprekend in overeenstemming zijn met artikel 14 van het Europees Verdrag voor de Rechten van de Mens, de artikelen 10 en 11 van de Grondwet en de wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie.

Elke zorggebruiker heeft steeds het recht een vaccinatieattest te verkrijgen. Dit kan evenwel nooit leiden tot een discriminatie ten aanzien van de zorggebruikers » (*Belgisch Staatsblad* van 12 april 2021, pp. 32404-32408; zie ook *Parl. St.*, Kamer, 2020-2021, DOC 55-1853/001, pp. 9-13).

B.20.2. In haar advies over het voorontwerp van wet dat de wet van 2 april 2021 houdende instemming met het samenwerkingsakkoord van 12 maart 2021 is geworden, heeft de afdeling wetgeving van de Raad van State met betrekking tot de doeleinden van de gegevensverwerking opgemerkt :

« In paragraaf 2, 9°, wordt als verwerkingsdoeleinde vermeld

‘ de verdeling van de kosten van de vaccinatie tussen de Federale Staat en de gefedereerde entiteiten, na anonimisering van de gegevens of ten minste pseudonimisering van de gegevens voor het geval dat de anonimisering de berekening van de verdeling niet mogelijk zou maken ’.

Overeenkomstig het beginsel van de minimale gegevensverwerking mag niet worden voorzien in de mogelijkheid van pseudonimisering indien de registratie van geanonimiseerde gegevens volstaat om het nagestreefde doel te bereiken.

Naar aanleiding van de vraag in welke gevallen de anonimisering van de gegevens het niet mogelijk zou maken om de verdeling van de kosten van de vaccinatie te berekenen, preciseerden de gemachtigden het volgende :

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

Op basis van dat antwoord is het onmogelijk uitspraak te doen over de vraag of de onderzochte bepaling aanvaard kan worden. De steller van het voorontwerp wordt dan ook verzocht in de toelichting bij dit artikel te preciseren in welke gevallen de anonimisering van de gegevens het niet mogelijk zou maken om de verdeling van de kosten van de vaccinatie te berekenen » (*ibid.*, pp. 51-52; zie ook *Parl. St.*, Vlaams Parlement, 2020-2021, nr. 708/1, p. 88; *Parl. St.*, Waals Parlement, 2020-2021, nr. 509/1, p. 84; *Parl. St.*, Parlement van de Duitstalige Gemeenschap, 2020-2021, nr. 132/1, pp. 31-32; *Parl. St.*, Verenigde Vergadering van de Gemeenschappelijke Gemeenschapscommissie, 2020-2021, nr. B-65/1, pp. 16-17; *Parl. St.*, Vergadering van de Franse Gemeenschapscommissie, 2020-2021, nr. 45/1, p. 32).

B.20.3. In haar advies nr. 16/2021 van 10 februari 2021 betreffende het ontwerp van samenwerkingsakkoord dat het samenwerkingsakkoord van 12 maart 2021 is geworden, heeft de Gegevensbeschermingsautoriteit opgemerkt :

« 33. Minstens volgende ruim geformuleerde doeleinden nopen (nog steeds) bijkomende afbakening en precisering :

- ‘ het verstrekken van gezondheidszorg en behandelingen, zoals bedoeld in artikel 9.2, h) AVG ’,

- ‘ monitoring en surveillance na vergunning van de vaccins overeenkomstig de goede praktijken aanbevolen door de Wereldgezondheidsorganisatie ’,

- ‘ uitvoeren van wetenschappelijke of statistische studies ’,

- evenals het nieuw in het ontwerp van samenwerkingsakkoord opgedoken doeleinde ‘ het informeren en sensibiliseren van zorggebruikers met betrekking tot de COVID-19 vaccinatie door zorgverleners ’.

34. In navolging van de opmerking van de Autoriteit in advies nr. 138/2020 (randnr. 34), worden in artikel 4, § 2, 2° en 3° van het ontwerp van samenwerkingsakkoord de doeleinden ‘ geneesmiddelenbewaking van de vaccins tegen COVID-19 ’ en ‘ traceerbaarheid van de vaccins tegen COVID-19 ’ aangevuld met de terzake geldende regelgeving. De Autoriteit neemt er akte van.

35. Ingevolge artikel 4, § 2, 4° en 5° van het ontwerp van samenwerkingsakkoord moeten de in Vaccinnet geregistreerde gegevens (waaronder een belangrijk aandeel gevoelige gezondheidsgegevens) ook toelaten vaccinatiemomenten in te plannen evenals de logistieke organisatie van de vaccinatie tegen COVID-19. De Autoriteit kan zich echter niet van de indruk ontdoen dat de met het ontwerp van samenwerkingsakkoord in het leven geroepen ‘ gegevensbank met vaccinatiecodes ’ (waarin omzeggens geen (op de vaccinatiestatus na) gevoelige gezondheidsgegevens worden opgenomen) net tot doel had het organisatorische en logistieke luik van plannen en uitnodigen voor vaccinatiemomenten af te dekken (zoals ook blijkt uit artikel 4, § 1, 1° en 2° van het ontwerp van samenwerkingsakkoord). *Quid* ? Betreft de dubbele vermelding (artikel 4, § 1, 1° en § 2, 4°) van een (tekstueel) zelfde doeleinde (beheer van vaccinatieschema’s en inplannen vaccinatiemomenten) mogelijks een vergissing ?

36. In advies nr. 138/2020 merkte de Autoriteit (in randnr. 35) op dat het ‘ bepalen van de vaccinatiegraad tegen COVID-19 ’ een statistisch doeleinde lijkt dat kan worden gerealiseerd aan de hand van anonieme gegevens (of minstens gepseudonimiseerde persoonsgegevens voor zover anonimisering het bepalen van de vaccinatiegraad niet zou toelaten). De Autoriteit adviseerde dienvolgens zulks uitdrukkelijk in het ontwerp toe te voegen. De Autoriteit stelt vast dat terzake enkel in de Memorie van toelichting het woord ‘ anoniem ’ werd toegevoegd; zij dringt niettemin aan (naar analogie met andere doeleinden die kunnen gerealiseerd worden aan de hand van anonieme/minstens gepseudonimiseerde gegevens) zulks in de tekst van het ontwerp van samenwerkingsakkoord zelf op te nemen.

37. In navolging van de vraag terzake van de Autoriteit in advies nr. 138/2020 (randnr. 36) vult artikel 4, § 2, 7° van het ontwerp van samenwerkingsakkoord het doeleinde van ‘ het organiseren van de contactopsporing ’ aan met een uitdrukkelijke verwijzing naar ’ in uitvoering van het Samenwerkingsakkoord van 25 augustus 2020 (...)[’].

In de Memorie van Toelichting wordt het belang van de link met contactopsporing aan de hand van volgende scenario’s toegelicht :

- ‘ het advies dat door het contactcenter dient te worden gegeven kan verschillen naargelang iemand al dan niet gevaccineerd is;

- de bron is gevaccineerd maar heeft een aantal contacten besmet; dit betreft een geval van vaccin failure of een variant strain waar het vaccin niet tegen beschermt en dus heel belangrijke informatie voor de volksgezondheid;

- de bron is niet gevaccineerd, waardoor anderen besmet geraakt zijn;

- contacten kunnen gevaccineerd zijn, waardoor de epidemie uitdooft;

- contacten zijn niet gevaccineerd, waarbij de epidemie verder actief in kaart moet worden gebracht. ’[.]

38. De Autoriteit neemt akte van deze toelichting en begrijpt de meerwaarde van informatie inzake vaccinatiestatus voor contactopsporing. Zij acht het weliswaar aangewezen in het ontwerp van samenwerkingsakkoord te preciseren welke gegevens dienvolgens vanuit Vaccinnet zullen worden geëxporteerd naar de Gegevensbank(en) van Sciensano, minstens de nodige wijzigingen door te voeren in de bepalingen van het Samenwerkingsakkoord van

25 augustus 2020 waarin de gegevenscategorieën van de daarin omkaderde Gegevensbank(en) en hun bronnen worden beschreven. Een gebeurlijke beraadslaging van het Informatieveiligheidscomité met betrekking tot dergelijke gegevensstroom moet immers stroken met wat de regelgeving terzake, inzonderheid onderhavig ontwerp van samenwerkingsakkoord en meer nog het samenwerkingsakkoord van 25 augustus 2020 op dat vlak voorschrijven.

39. Artikel 4, § 2, 10° van het ontwerp van samenwerkingsakkoord vermeldt dat wetenschappelijke of statistische studies zullen worden uitgevoerd ' in overeenstemming met titel 4 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens '. De Autoriteit wijst erop dat titel 4 van de WVG uitvoering geeft aan artikel 89, §§ 2 en 3 AVG en dienvolgens het uitzonderingsregime bepaalt voor onderzoek dat enkel kan worden verwezenlijkt met beperkingen/afwijkingen op de rechten van betrokkenen zoals vermeld in artikelen 15 e.v. van de AVG. *Quid* ?

40. In artikel 4, § 2, 11° van het ontwerp van samenwerkingsakkoord duikt voor het eerst een nieuw - met de vaccinatieregistratie in Vaccinnet - na te streven doeleinde op, meer bepaald : ' het informeren en sensibiliseren van zorggebruikers met betrekking tot de COVID-19 vaccinatie door zorgverleners '. Het is voor de Autoriteit volstrekt onduidelijk in welke mate de verwezenlijking van een doeleinde als ' informeren en sensibiliseren voor COVID-19-vaccinatie ' nood heeft aan persoonsgegevens. Wanneer het de bedoeling is ' gepersonaliseerd ' te informeren en sensibiliseren van burgers die een vaccin weigeren, moet zulks ook als dusdanig klaar en duidelijk in het ontwerp van samenwerkingsakkoord worden gepreciseerd, teneinde de betrokken parlementen zulks met kennis van zaken al dan niet te laten aanvaarden. Grootschalige sensibilisering[s]campagnes (van bepaalde doelgroepen) kunnen volgens de Autoriteit perfect aan de hand van anonieme gegevens ».

B.20.4. De minister van Volksgezondheid heeft gepreciseerd dat « het samenwerkingsakkoord enkel betrekking heeft op de vaccinatiecampagne in de strijd tegen COVID-19 en dat de gegevens niet voor andere doeleinden gebruikt mogen worden », andere dan die welke « uitsluitend te maken [hebben] met de vaccinatiecampagne » (*Parl. St.*, Kamer, 2020-2021, DOC 55-1853/002, p. 12).

B.21.1. Krachtens het beginsel van minimale gegevensverwerking moeten persoonsgegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (artikel 5, lid 1, c), van de AVG).

B.21.2. Zoals in B.16.4 is vermeld, omvat het recht op eerbiediging van het privéleven de bescherming van persoonsgegevens en van persoonlijke informatie waartoe met name de naam en de gezondheidsgegevens behoren.

De bestreden akten, waarbij instemming wordt verleend met bepalingen die voorzien in de verwerking van persoonsgegevens, met inbegrip van gevoelige gegevens over gezondheid, in de gegevensbank « Vaccinnet », leiden tot een inmenging in het recht op bescherming van persoonsgegevens, dat wordt gewaarborgd door de in B.16 aangehaalde bepalingen.

In artikel 4, lid 15, van de AVG worden « gegevens over gezondheid » gedefinieerd als « persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven ». Aangezien de in de gegevensbank « Vaccinnet » geregistreerde gegevens met name betrekking hebben op gegevens over gezondheid in de zin van de voormelde bepaling, moeten zij worden verwerkt overeenkomstig artikel 9 van de AVG.

Artikel 9, lid 1, van de AVG verbiedt in beginsel de verwerking van gevoelige persoonsgegevens, zoals gegevens over gezondheid. Artikel 9, lid 2, h), van de AVG staat een dergelijke verwerking evenwel toe wanneer zij noodzakelijk is « voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker » en wanneer zij onderworpen is aan het beroepsgeheim. Artikel 9, lid 2, i), van de AVG bepaalt dat de verwerking van dergelijke gegevens ook is toegestaan wanneer zij noodzakelijk is « om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim ».

In overweging 54 van de AVG wordt in dat verband vermeld :

« Het kan om redenen van algemeen belang op het gebied van de volksgezondheid nodig zijn om bijzondere categorieën van persoonsgegevens zonder toestemming van de betrokkene te verwerken. Die verwerking moet worden onderworpen aan passende en specifieke maatregelen ter bescherming van de rechten en vrijheden van natuurlijke personen. In dit verband dient ' volksgezondheid ' overeenkomstig de definitie van Verordening (EG) nr. 1338/2008 van het Europees Parlement en de Raad te worden uitgelegd als alle elementen in verband met de gezondheid, namelijk gezondheidstoestand, inclusief morbiditeit en beperkingen, de determinanten die een effect hebben op die gezondheidstoestand, de behoeften aan gezondheidszorg, middelen ten behoeve van de gezondheidszorg, de verstrekking van en de universele toegang tot gezondheidszorg, alsmede de uitgaven voor en de financiering van de gezondheidszorg, en de doodsoorzaken. Dergelijke verwerking van persoonsgegevens over gezondheid om redenen van algemeen belang mag er niet toe [...] leiden dat persoonsgegevens door derden zoals werkgevers, of verzekeringsmaatschappijen en banken voor andere doeleinden worden verwerkt ».

B.21.3. Krachtens het beginsel van doelbinding moeten persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en moet de eventuele verdere verwerking van die gegevens verenigbaar zijn met die oorspronkelijke doeleinden (artikel 5, lid 1, b), van de AVG).

Zoals in B.16.9 en B.16.10 is vermeld, moet eenieder, krachtens het wettigheidsbeginsel, een voldoende duidelijk beeld hebben van de doeleinden van de verwerking van de gegevens die op hem betrekking hebben.

B.22.1. Met de bestreden akten wordt een legitiem doel nagestreefd dat erin bestaat de verspreiding tegen te gaan van het coronavirus SARS-CoV-2, dat een zeer besmettelijk virus is dat overdraagbaar is via de lucht. De COVID-19-pandemie wordt gekenmerkt door een hoog reproductiegetal. Zonder sanitaire maatregelen kent dat virus een zeer snelle exponentiële verspreiding.

Zoals in B.2 is vermeld, past de registratie van de vaccinatiegegevens, enerzijds, in het kader van de Belgische vaccinatiestrategie die is vastgesteld op grond van de wetenschappelijke gegevens inzake COVID-19-vaccins, zoals zij beschikbaar waren op het ogenblik dat de bestreden akten werden aangenomen, teneinde de COVID-19-pandemie te bestrijden door de besmettingen met het coronavirus COVID-19 te verminderen, alsook, anderzijds, in het kader van de inzet op Europees niveau van een digitaal EU-COVID-certificaat, op grond onder meer van de bekommernis om interoperabiliteit van de vaccinatiecertificaten.

In die context is de registratie van de vaccinatiegegevens onontbeerlijk voor het nastreven van die doelstellingen, en maakt de centralisatie van de registratie van die gegevens het mogelijk om « het geschikte doseringsschema te bepalen, met name wat de verschillende doses van een toe te dienen vaccin betreft (juiste interval in geval van een vaccin met meerdere dosissen), en strekt zij ertoe de goede werking van de massale vaccinatiecampagne tegen COVID-19 te verzekeren » (*Parl. St.*, Waals Parlement, 2020-2021, nr. 509/1, p. 3).

Een dergelijke maatregel beoogt dan ook de gezondheid van anderen en de volksgezondheid alsook de rechten en vrijheden van anderen te waarborgen.

B.22.2. In het samenwerkingsakkoord van 12 maart 2021 worden, in die context, uitdrukkelijk elf doeleinden vastgesteld waarvoor de in artikel 3, § 2, vermelde persoonsgegevens worden verzameld en verwerkt in de gegevensbank « Vaccinnet », en in de algemene toelichting bij het samenwerkingsakkoord van 12 maart 2021 wordt uitdrukkelijk gepreciseerd dat die gegevens « niet voor andere doeleinden dan die voorzien in dit akkoord [mogen] worden gebruikt », « in het bijzonder maar niet uitsluitend politionele, commerciële, fiscale, strafrechtelijke of [aan staatsveiligheid verbonden doeleinden] » (*Belgisch Staatsblad* van 12 april 2021, p. 32407).

Door de bestreden akten aan te nemen, hebben de verschillende bevoegde wetgevers, overeenkomstig hetgeen in B.16.9 en B.16.10 is vermeld, zelf de essentiële elementen van de verwerking van persoonsgegevens geregeld, door de doeleinden van de verwerking van de in de gegevensbank « Vaccinnet » opgenomen gegevens exhaustief te omschrijven.

Daarenboven worden in de algemene toelichting bij het samenwerkingsakkoord van 12 maart 2021 tal van preciseringen verschaft over de doeleinden, waardoor aldus een antwoord wordt geboden op de kritiek die door de Gegevensbeschermingsautoriteit is geformuleerd in haar in B.20.3 aangehaalde advies.

B.23.1. Om het welbepaalde karakter van de in artikel 4, § 2, van het samenwerkingsakkoord bedoelde doeleinden te onderzoeken, dient het Hof, in de in B.2 in herinnering gebrachte context, rekening te houden met het intrinsiek evolutieve karakter van de wetenschappelijke kennis met betrekking tot de specifieke kenmerken van het coronavirus SARS-CoV-2 en de mogelijke mutaties ervan, maar ook met de doeltreffendheid van de vaccins die kort vóór de start van de vaccinatiecampagne in de handel zijn gebracht en met de doeltreffendheid ervan op middellange en lange termijn.

B.23.2.1. Uit de in B.20 aangehaalde parlementaire voorbereiding blijkt dat de elf doeleinden die in artikel 4, § 2, zijn omschreven, rechtstreeks verband houden met de massale vaccinatiecampagne die op nationaal niveau is gevoerd, op grond van de wetenschappelijke kennis die beschikbaar was op het ogenblik van de start van die campagne.

Het loutere feit dat er elf doeleinden van een gegevensverwerking zijn, maakt het niet mogelijk om, zoals de verzoekende partij aanvoert, te besluiten dat die doeleinden op zich buitensporig zouden zijn. Het welbepaalde karakter van een doeleinde moet immers worden beoordeeld op grond van de voorliggende omstandigheden en het expliciteren van de verschillende doeleinden kan een waarborg vormen voor de gegevensverwerking (advies 03/2013 over doelbinding, 2 april 2013, Groep gegevensbescherming artikel 29, p. 15).

B.23.2.2. Aldus zijn de doeleinden « geneesmiddelenbewaking van de vaccins tegen COVID-19 » (2°), « traceerbaarheid van de vaccins » (3°), « beheren van schema's voor vaccinatie » (4°), « logistieke organisatie van de vaccinatie tegen COVID-19 » (5°), « bepalen van de anonieme vaccinatiegraad tegen COVID-19 van de bevolking » (6°) en « uitvoeren van de monitoring en surveillance na vergunning van de vaccins » (8°) precies en houden zij rechtstreeks verband met de organisatie van de op nationaal niveau gevoerde massale vaccinatiecampagne tegen COVID-19.

Die verschillende elementen zijn immers noodzakelijk om de logistieke organisatie van de vaccinatie te regelen, rekening houdend met de verschillende doelgroepen die moeten worden uitgenodigd en met het aantal toe te dienen doses, maar ook om de vaccinatiegraad te beoordelen, te evalueren in welke mate het vaccin een immuniteitsrespons kan opwekken en de eventuele ongewenste bijwerkingen van dat vaccin te detecteren. De monitoring en surveillance van de vaccins na vergunning worden geregeld overeenkomstig de goede praktijken van de Wereldgezondheidsorganisatie ter zake. In het kader van het doeleinde « geneesmiddelenbewaking van de vaccins » voorziet artikel 45 van de wet van 13 juni 2021 « houdende maatregelen ter beheersing van de COVID-19-pandemie en andere dringende maatregelen in het domein van de gezondheidszorg » in het opnemen van in « Vaccinnet » vermelde gegevens in een federale databank, waarvan het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten de verwerkingsverantwoordelijke is.

In tegenstelling tot hetgeen de verzoekende partij aanvoert, werd het doeleinde met betrekking tot het « verstrekken van gezondheidszorg en behandelingen » in artikel 4, § 2, 1°, van het samenwerkingsakkoord van 12 maart 2021 uitdrukkelijk in die zin beperkt dat het « uitsluitend [...] de vaccinatie en de ondersteunings-, de informatie- en de sensibiliseringsmaatregelen ten aanzien van de burgers voor wat de vaccinatie betreft » beoogt, onder verwijzing naar artikel 9, lid 2, h), van de AVG. Er werd eveneens gepreciseerd dat dat doeleinde geenszins beoogt « de toegang tot kwalitatieve zorgverstrekking op enige manier [te] beperken of afhankelijk [te] stellen in functie van de vaccinatiestatus van een persoon » (algemene toelichting bij het samenwerkingsakkoord van 12 maart 2021, *Belgisch Staatsblad* van 12 april 2021, p. 32407). Daaruit vloeit voort dat dat doeleinde eveneens precies is en rechtstreeks verband houdt met de vaccinatie tegen COVID-19 en met de medische monitoring van de gevaccineerde persoon.

Het in artikel 4, § 2, 1°, bedoelde doeleinde houdt aldus eveneens verband met het in artikel 4, § 2, 10°, bedoelde doeleinde « uitvoeren van wetenschappelijke of statistische studies », alsook met het in artikel 4, § 2, 11°, bedoelde doeleinde betreffende « het informeren en sensibiliseren van personen met betrekking tot de COVID-19 vaccinatie ». Uit de beginselen waartoe inzake de vaccinatiestrategie is beslist, blijkt immers dat België ernaar streeft een vorm van groepsimmuniteit via een voldoende vaccinatiegraad van 70 % van de bevolking te bereiken. De verwerking van gegevens met het oog op wetenschappelijk en statistisch onderzoek wordt met name beoogd in artikel 89, lid 1, van de AVG, dat voorziet in het beginsel van minimale gegevensverwerking, met name pseudonimisering waarin minstens wordt voorzien in artikel 4, § 2, 10°, voor het geval dat anonimisering het niet mogelijk zou maken de wetenschappelijke of statistische studie uit te voeren. In dat verband werd beklemtoond dat een « hoge vaccinatiegraad binnen de bevolking een belangrijke en fundamentele uitdaging op het vlak van volksgezondheid vormt ten aanzien van de ongeziene COVID-19-pandemie, terwijl het op het niveau van het individu ook belangrijk is dat de betrokkene een geïnformeerde keuze kan maken voor zijn persoonlijke gezondheid » (algemene toelichting bij het samenwerkingsakkoord van 12 maart 2021, *Belgisch Staatsblad* van 12 april 2021, p. 32407), zodat statistische studies over die vaccinatiegraad noodzakelijk zijn. Studies over de vaccinatiegraad maken het mogelijk om het percentage gevaccineerde personen in specifieke risicogroepen in te schatten en helpen om in het vaccinatieprogramma eventuele lacunes vast te stellen die zouden moeten worden weggewerkt, in voorkomend geval door gericht te informeren en te sensibiliseren, door middel van algemene campagnes of individueel, op grond van de vastgestelde houding van de bevolking. Het feit dat de vaccinatie op vrijwillige basis geschiedt, maakt het doeleinde « informeren en sensibiliseren » noodzakelijk ten aanzien van het doel een voldoende vaccinatiegraad te bereiken. Op grond van die kennis kan de rol van de arts bij die gerichte informatie belangrijk blijken te zijn, ook al is het verboden om personen te contacteren die uitdrukkelijk hebben verklaard dat zij het vaccin weigeren (*ibid.*).

B.23.2.3. Het doeleinde met betrekking tot de « contactopsporing » (7°) houdt verband met het feit dat de vaccinatiestatus, binnen de exclusieve doelstelling van het onderzoek van besmettelijke contacten, het besmettingsrisico rechtstreeks beïnvloedt. De gegevens die in dat kader vanuit « Vaccinnet » naar de gegevensbank van Sciensano worden overgedragen, zijn beperkt, maar « flexibiliteit blijft noodzakelijk op basis van evoluerende wetenschappelijke inzichten inzake de impact van vaccinatie op besmettingsrisico's » (*ibid.*, p. 32406).

B.23.2.4. Het doeleinde met betrekking tot de « berekening van de verdeling van de kosten voor de vaccinatie » (9°) tussen de federale overheid en de deelentiteiten houdt verband met het feit dat de kosteloze vaccinatiecampagne werd georganiseerd via een samenwerkingsakkoord tussen de bevoegde overheden, en dat de partijen bij dat akkoord die vaccinatie moeten financieren.

Het feit dat de gegevens, zoals de afdeling wetgeving van de Raad van State beklemtoont, mogelijk niet worden geanonimiseerd maar enkel worden gepseudonimiseerd, kan worden verantwoord, zoals in de algemene toelichting bij het samenwerkingsakkoord wordt vermeld ten aanzien van de anonieme vaccinatiegraad tegen COVID-19, door het feit dat anonimisering het nagestreefde doel mogelijk niet kan bereiken (*ibid.*, p. 32407), maar artikel 4, § 2, 8°, waarborgt dat de desbetreffende gegevens minstens zullen worden gepseudonimiseerd. Op grond van dat doeleinde heeft het protocolakkoord van 9 februari 2022 tussen de federale Regering en de in artikel 128, 130 en 135 van de Grondwet bedoelde overheden « inzake de cofinanciering van het COVID-19 vaccinatieprogramma » de kosten voor de vaccinatie tegen COVID-19 verdeeld tussen de verschillende overheden.

Wat de anonimisering of de pseudonimisering betreft, moet worden vastgesteld dat het om technische en organisatorische maatregelen gaat die moeten worden genomen om de verwerking van persoonsgegevens te beschermen, maar die allebei waarborgen dat de identiteit van de betrokken persoon niet zal worden onthuld. Sommige elementen kunnen immers « fijnmazig » moeten worden bepaald : in de algemene toelichting bij het samenwerkingsakkoord van 12 maart 2021 wordt in dat verband het voorbeeld vermeld van de woonzorgcentra waarin een onderscheid moet worden gemaakt tussen zorgpersoneel en residenten (*ibid.*, p. 32407). De evolutie van de omstandigheden en van de epidemiologische werkelijkheid kan immers vereisen dat de situatie veeleer door de ene maatregel dan door de andere wordt geregeld, zonder dat de mogelijkheid om gebruik te maken van een van beide maatregelen kan worden beschouwd als een nalatigheid wat betreft het bepalen van een essentieel element van de doeleinden van de gegevensverwerking.

B.23.3. Uit het voorgaande vloeit voort dat de in artikel 4, § 2, van het samenwerkingsakkoord omschreven doeleinden rechtstreeks verband houden met de op nationaal niveau gevoerde massale vaccinatiecampagne, voldoende precies en welbepaald zijn en zich beperken tot wat strikt noodzakelijk is in verband met die vaccinatie.

B.24. Doordat het is gericht tegen de bestreden akten in zoverre daarbij instemming wordt verleend met artikel 4, § 2, van het samenwerkingsakkoord, is het eerste onderdeel van het enige middel, niet gegrond.

II. Wat betreft de in artikel 5 bedoelde machtiging aan het Informatieveiligheidscomité om de mededeling van persoonsgegevens aan derden toe te staan (eerste onderdeel)

B.25.1. In het eerste onderdeel van het middel is de verzoekende partij van mening dat de in artikel 5 van het samenwerkingsakkoord van 12 maart 2021 vastgestelde categorieën van ontvangers van de persoonsgegevens onvoldoende waarborgen inzake voorzienbaarheid bieden. Bovendien wordt bij artikel 5, derde lid, van het samenwerkingsakkoord van 12 maart 2021 aan het Informatieveiligheidscomité de bevoegdheid gedelegeerd om essentiële elementen te bepalen, namelijk de derde instanties die de verzamelde gegevens kunnen verwerken, alsook de doeleinden van de verwerking van die gegevens.

B.25.2. Zoals in B.10.1 is vermeld, hebben de grieven van de verzoekende partij enkel betrekking op de gegevensbank « Vaccinnet », zodat het Hof het middel dat tegen artikel 5 van het samenwerkingsakkoord van 12 maart 2021 is gericht, enkel onderzoekt in zoverre het betrekking heeft op de mededeling van de in artikel 3, § 2, van het voormelde samenwerkingsakkoord bedoelde gegevens die in de gegevensbank « Vaccinnet » zijn geregistreerd.

B.26.1. Artikel 5 van het samenwerkingsakkoord van 12 maart 2021 bepaalt :

« Met als uitsluitend doel de in artikel 4 opgesomde doeleinden te realiseren, mogen de in artikel 3 bedoelde persoonsgegevens worden meegedeeld aan personen of instanties die zijn belast met een taak van algemeen belang door of krachtens een wet, een decreet of een ordonnantie op voorwaarde dat deze mededeling noodzakelijk is voor de uitvoering van de opdracht van algemeen belang van de betrokken personen of instanties en dat enkel de nodige gegevens gelet op de doeleinden van artikel 4 worden meegedeeld.

De in artikel 3 bedoelde persoonsgegevens worden meegedeeld aan onderzoeksinstellingen indien ze noodzakelijk zijn voor wetenschappelijk of statistisch onderzoek, na anonimisering of op zijn minst pseudonimisering van de gegevens voor het geval dat anonimisering niet zou toelaten het wetenschappelijk of statistisch onderzoek uit te voeren.

Elke gegevensmededeling vereist een beraadslaging van de kamer ' sociale zekerheid en gezondheid ' van het informatieveiligheidscomité teneinde de naleving van de in dit artikel vermelde voorwaarden te kunnen nagaan.

Het Informatieveiligheidscomité publiceert op het eGezondheidsportaal een precieze functionele beschrijving van de informatiesystemen die worden opgezet voor de uitvoering van dit samenwerkingsakkoord en de informatiestromen tussen deze informatiesystemen die het voorwerp hebben uitgemaakt van een beraadslaging van het Informatieveiligheidscomité, inzonderheid met betrekking tot de informatieverwerking, de processen en de gegevensbanken.

De beraadslagingen van het Informatieveiligheidscomité worden systematisch gepubliceerd op de website van het eHealth-platform ».

B.26.2. Wat betreft de in artikel 5 bedoelde mededeling van gegevens aan derden wordt in de algemene toelichting bij het samenwerkingsakkoord van 12 maart 2021 vermeld :

« Met als uitsluitend doel de in artikel 4 opgesomde doeleinden te realiseren, mogen de in artikel 3 bedoelde persoonsgegevens worden meegedeeld aan personen of instanties die zijn belast met een taak van algemeen belang door of krachtens een wet, een decreet of een ordonnantie op voorwaarde dat deze mededeling noodzakelijk is voor de uitvoering van de opdracht van algemeen belang van de betrokken personen of instanties en dat enkel de nodige gegevens gelet op de doeleinden van artikel 4 worden meegedeeld.

De in artikel 3 bedoelde persoonsgegevens worden na anonimisering of op zijn minst pseudonimisering van de gegevens meegedeeld aan onderzoeksinstellingen indien ze noodzakelijk zijn voor wetenschappelijk of statistisch onderzoek. (terminologie van artikel 89 van de Algemene Verordening Gegevensbescherming).

Elke gegevensmededeling vereist een beraadslaging van de kamer ' sociale zekerheid en gezondheid ' van het informatieveiligheidscomité teneinde de naleving van de in dit artikel vermelde voorwaarden te kunnen nagaan.

Het Informatieveiligheidscomité kan enkel beraadslagingen verlenen voor concrete gegevensuitwisselingen binnen het kader van huidig samenwerkingsakkoord en dus in geen geval zelf andere verwerkingsdoeleinden noch categorieën van persoonsgegevens vaststellen. Het is geenszins bevoegd om een essentieel element van de verwerking van persoonsgegevens te bepalen, overeenkomstig het principe van wettelijkheid zoals bepaald in artikel 22 van de Grondwet. Het is dus niet belast met een dergelijke opdracht op grond van dit samenwerkingsakkoord.

Het Informatieveiligheidscomité publiceert op het eGezondheidsportaal een precieze functionele beschrijving van de informatiesystemen die worden opgezet voor de uitvoering van dit akkoord en de informatiestromen tussen deze informatiesystemen die het voorwerp hebben uitgemaakt van een beraadslaging van het Informatieveiligheidscomité inzonderheid met betrekking tot de informatieverwerking, de processen en de gegevensbanken.

Daarnaast worden de beraadslagingen van het Informatieveiligheidscomité systematisch gepubliceerd op de website van het eHealth-platform. De beraadslagingen van het informatieveiligheidscomité bevatten steeds de verschillende aspecten die nodig zijn voor het beoordelen van de eerbiediging van de regelgeving inzake de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens (in het bijzonder de Algemene Verordening Gegevensbescherming). Aldus worden telkens uitdrukkelijk de betrokken partijen (verwerkingsverantwoordelijken) vermeld, alsmede de door hen beoogde doeleinden en een (doorgaans exhaustief) overzicht van de persoonsgegevens die voor diezelfde doeleinden moeten worden verwerkt. Het informatieveiligheidscomité gaat onder meer na of de verwerking van persoonsgegevens rechtmatig is (en dus beantwoordt aan één van de voorwaarden van artikel 6 van de GDPR) en de basisbeginselen worden gerespecteerd (doelbinding, minimale gegevensverwerking, opslagbeperking en informatieveiligheid).

Het gebruik van een gemeenschappelijke gegevensbank sluit niet uit dat verschillende, eventueel gefedereerde entiteit-specifieke eindgebruikersinterfaces worden gebruikt voor het voeden of raadplegen van de gemeenschappelijke gegevensbank.

Het is belangrijk erop te wijzen dat de gegevens die op grond van dit akkoord worden ingezameld slechts in twee gevallen mogen worden meegedeeld, die op strikt limitatieve wijze zijn vastgesteld :

- ofwel is de derde, op cumulatieve wijze, belast met een opdracht van algemeen belang en is die gemachtigd om dergelijke gegevens te verwerken door of krachtens een wet, decreet of ordonnantie die uitdrukkelijk een doeleinde beoogt waarin voorzien wordt door dit akkoord;

- ofwel is de derde een onderzoeksinstelling voor wetenschappelijke en statistische studies. In dat geval worden enkel geanonimiseerde gegevens meegedeeld of gepseudonimiseerde gegevens ingeval de anonimisering niet toelaat om het doeleinde te bereiken.

Onder derden kunnen onder meer de zorgverstrekkers, die een therapeutische relatie hebben met de zorggebruiker, en de verzekeringsinstellingen worden begrepen, vanzelfsprekend binnen de grenzen van hun respectievelijke opdrachten.

Indien het niet mogelijk of niet relevant is om deze derden bij name aan te wijzen in een samenwerkingsakkoord, zullen deze criteria niettemin toelaten om de betrokken categorieën van derden te omkaderen en strikt te beperken. De rol van het Informatieveiligheidscomité is er voorts op gericht een bijkomende filter toe te voegen om ervoor te zorgen dat de gegevensstroom wel degelijk kadert binnen de beoogde doelstelling en binnen de wens om de mededeling van dergelijke gegevens zoveel mogelijk te beperken. Daarbij biedt het de nodige flexibiliteit (door geen stromen van evolutieve gegevens uit te sluiten bijvoorbeeld) en versterkt het de waarborgen op het vlak van bescherming van de privacy door een feitelijke controle. Er wordt immers vermeden dat een automatische stroom wordt gegenereerd zonder dat er voorafgaandelijk wordt gecontroleerd of die effectief is toegelaten. Zoals de Gegevensbeschermingsautoriteit benadrukt in haar advies 16-2021 van 18 februari 2021, biedt een beraadslaging van het Informatieveiligheidscomité een meerwaarde door de uitvoeringsmodaliteiten nader te bepalen, onder meer op het vlak van informatieveiligheid en proportionaliteit beoogd door de wet.

In antwoord op het advies van de Raad van State 68/844/VR van 18 februari 2021 en gelet op het voorgaande, wordt erop gewezen dat het voorleggen van de mededeling van persoonsgegevens aan een beraadslaging van het Informatieveiligheidscomité een door de federale wet vastgestelde regel is en een maatregel van gegevensbescherming door ontwerp en door standaardinstellingen vormt in de zin van de Algemene Verordening Gegevensbescherming. Het is gebaseerd op de artikelen 6, § 2 en 9, § 4 van de Algemene Verordening Gegevensbescherming.

In de beraadslagingen van het Informatieveiligheidscomité wordt namelijk gespecificeerd welke informatiebeveiligingsmaatregelen door de actoren van een gegevensmededeling moeten worden nageleefd en wordt preventief beoordeeld of er niet meer persoonsgegevens aan de verwervende organisatie worden verstrekt dan strikt nodig is om de legitieme doeleinden van de verwerking te verwezenlijken.

De beraadslagingen van het Informatieveiligheidscomité zijn bindend voor de actoren van de gegevensuitwisseling. Anderzijds hebben zij tot doel de actoren van de gegevensuitwisseling rechtszekerheid te bieden, zodat een effectieve en efficiënte gegevensuitwisseling niet onnodig wordt belemmerd door een gebrek aan duidelijkheid over de ten uitvoer te leggen informatiebeveiligingsmaatregelen of over de legitimiteit van de openbaarmaking van persoonsgegevens.

De beraadslagingen van het Informatieveiligheidscomité hebben alleen betrekking op de (elektronische) uitwisseling van gegevens. Bij zijn beraadslagingen is het Informatieveiligheidscomité gebonden aan de wettelijke bepalingen betreffende de verwerkingsdoeleinden van de instanties die de gegevens ontvangen. De beraadslagingen van het Informatieveiligheidscomité maken slechts een rechtsgrond uit, die een orgaan dat persoonsgegevens verwerkt op basis van legitieme doeleinden in staat stelt om deze persoonsgegevens aan andere organen mee te delen, in het kader van legitieme doeleinden waarvoor het ontvangende orgaan persoonsgegevens kan verwerken.

De beraadslagingen van het Informatieveiligheidscomité vormen geen rechtsgrondslag voor de eerste verzameling en verwerking van persoonsgegevens door de verstrekkende instantie. Ook de ontvangende instantie moet de persoonsgegevens verwerken op basis van de rechtsgronden die haar ter beschikking staan. Het Informatieveiligheidscomité kan derhalve de verwerkingsdoeleinden van de eerste verwerking door de gegevensverstrekkende instantie niet uitbreiden, noch kan het een rechtsgrondslag bieden voor andere doeleinden van verwerking door de ontvangende instantie dan die welke bij of krachtens de wet zijn voorzien. De beraadslagingen staan de uitwisseling van gegevens toe op voorwaarde dat de in de beraadslaging over het informatiebeveiligingsplan beschreven modaliteiten worden nageleefd en het evenredigheidsbeginsel wordt nageleefd, maar leggen dit niet op.

Het Informatieveiligheidscomité is geen toezichthoudende autoriteit in de zin van de Algemene Verordening Gegevensbescherming. Het is dus niet bevoegd om toezicht te houden op de naleving, problemen en geschillen op te lossen of klachten te behandelen. Het is inderdaad de Gegevensbeschermingsautoriteit die voor deze zaken bevoegd is. De Gegevensbeschermingsautoriteit kan te allen tijde elke beraadslaging van het Informatieveiligheidscomité vergelijken met hogere wettelijke normen en, in geval van niet-naleving, het Informatieveiligheidscomité verzoeken zijn beraadslaging over de door hem aangegeven punten te heroverwegen.

Het beroep op het Informatieveiligheidscomité moet aldus voor de betrokken partijen bij deze samenwerkingsovereenkomst niet worden opgevat als een afstand van bevoegdheid als gevolg van het toepassen van de regels » (*Belgisch Staatsblad* van 12 april 2021, pp. 32408-32411; zie ook *Parl. St.*, Kamer, 2020-2021, DOC 55-1853/001, pp. 13-16).

B.27.1. In haar advies over het voorontwerp van wet dat de wet van 2 april 2021 houdende instemming met het samenwerkingsakkoord van 12 maart 2021 is geworden, heeft de afdeling wetgeving van de Raad van State opgemerkt :

« Wat de mededeling aan derden betreft van persoonsgegevens afkomstig uit de gegevensbanken : luidens artikel 5, eerste lid, van het samenwerkingsakkoord moet het Informatieveiligheidscomité vooraf zijn goedkeuring verlenen voor elke mededeling van persoonsgegevens aan ' instanties met een opdracht van algemeen belang nodig voor de doeleinden waarmee deze instanties door of krachtens een wet, decreet of ordonnantie zijn belast en van deze gegevens na anonimisering, of minstens pseudonimisering aan de onderzoeksinstellingen voor wetenschappelijke of statistische studies '.

Gelet op de gevoelige aard van de persoonsgegevens die opgenomen zijn in de gegevensbanken, is een dergelijke beschrijving van de derden aan wie toegang verleend zou kunnen worden tot de gegevens te ruim. Het samenwerkingsakkoord moet nog nader gepreciseerd worden op dat punt » (*Parl. St.*, Kamer, 2020-2021, DOC 55-1853/001, p. 45; zie ook *Parl. St.*, Waals Parlement, 2020-2021, nr. 509/1, p. 81).

Voor zover het de bedoeling van de auteurs van het samenwerkingsakkoord zou zijn om een verordenende bevoegdheid te behouden voor de kamer « sociale zekerheid en gezondheid » van het Informatieveiligheidscomité, verwijst de afdeling wetgeving van de Raad van State naar de opmerking die is geformuleerd in het advies 67.719 van 15 juli 2020 over een voorontwerp dat de wet van 9 oktober 2020 « houdende instemming met het samenwerkingsakkoord van 25 augustus 2020 tussen de Federale Staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie, betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde gefedereerde entiteiten of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano » is geworden, over de (verordenende) bevoegdheden die aan de kamer « sociale zekerheid en gezondheid » van het Informatieveiligheidscomité waren gedelegeerd :

« 27. Bij de artikelen 11, § 3, en 12, § 1, van het samenwerkingsakkoord wordt voorzien in een delegatie van regelgevende bevoegdheid aan de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité, wat betreft bepaalde aspecten van de regeling van de verwerking van persoonsgegevens.

Het verlenen van verordenende bevoegdheid aan een openbare instelling, zoals het informatieveiligheidscomité, is in beginsel niet in overeenstemming met de algemene publiekrechtelijke beginselen omdat erdoor geraakt wordt aan het beginsel van de eenheid van de verordenende macht en een rechtstreekse parlementaire controle ontbreekt. Bovendien ontbreken de waarborgen waarmee de klassieke regelgeving gepaard gaat, zoals die inzake de bekendmaking, de preventieve controle van de Raad van State, afdeling Wetgeving, en de duidelijke plaats in de hiërarchie der normen. Dergelijke delegaties kunnen dan ook enkel worden gebillijkt voor zover zij zeer beperkt zijn en een niet-beleidsmatig karakter hebben, door hun detailmatige of hoofdzakelijk technische draagwijdte. De instellingen die de betrokken reglementering dienen toe te passen moeten hierbij zowel aan rechterlijke controle als aan politieke controle onderworpen zijn.

Daar komt nog bij dat het informatieveiligheidscomité een federale instelling is en dat een delegatie van regelgevende bevoegdheid aan een dergelijke instelling neerkomt op een afstand van bevoegdheden in hoofde van de deelstaten die bij het samenwerkingsakkoord betrokken zijn.

De conclusie is dan ook dat de beoogde delegaties aan het informatieveiligheidscomité moeten worden omgevormd tot delegaties aan een uitvoerend samenwerkingsakkoord, zoals in artikel 14, § 9, van het samenwerkingsakkoord, althans onder de voorwaarde dat geen nieuwe essentiële elementen van de verwerking van persoonsgegevens worden geregeld, maar hooguit de concretisering van hetgeen reeds voortvloeit uit het huidige samenwerkingsakkoord. Indien dat niet mogelijk is, moet het huidige samenwerkingsakkoord eerst worden aangevuld » (*ibid.*, pp. 52-54; zie ook *Parl. St.*, Vlaams Parlement, 2020-2021, nr. 708/1, pp. 88-89; *Parl. St.*, Waals Parlement, 2020-2021, nr. 509/1, p. 85; *Parl. St.*, Parlement van de Duitstalige Gemeenschap, 2020-2021, nr. 132/1, pp. 32-33; *Parl. St.*, Verenigde Vergadering van de Gemeenschappelijke Gemeenschapscommissie, 2020-2021, nr. B-65/1, pp. 17-18; *Parl. St.*, Vergadering van de Franse Gemeenschapscommissie, 2020-2021, nr. 45/1, p. 33).

B.27.2. In haar advies nr. 16/2021 van 10 februari 2021 over het voorontwerp van samenwerkingsakkoord dat het samenwerkingsakkoord van 12 maart 2021 is geworden, heeft de Gegevensbeschermingsautoriteit opgemerkt :

« 43. De Autoriteit neemt weliswaar akte van het feit dat artikel 5 van het ontwerp van samenwerkingsakkoord uitdrukkelijk verwijst naar diens artikel 4, § 3 (' De gegevens die in het kader van dit samenwerkingsakkoord worden ingezameld, mogen niet voor andere doeleinden dan die voorzien in dit akkoord worden gebruikt. ').

Aangezien de Autoriteit reeds in haar advies nr. 138/2020 en ook in onderhavig advies weerom vaststelt dat sommige in het ontwerp van samenwerkingsakkoord vermelde doeleinden dermate ruim zijn geformuleerd - waardoor ze niet beantwoorden aan de terzake geldende vereiste van welbepaald en uitdrukkelijk omschreven (zie artikel 5.1.b) AVG) - biedt de verwijzing in artikel 5 van het ontwerp van samenwerkingsakkoord naar artikel 4, § 3, onvoldoende garanties voor de betrokkenen op het vlak van voorzienbaarheid.

Zoals reeds aangehaald onder randnr. 10 van onderhavig advies, vereist het wettelijkheidsbeginsel dat een inmenging in het recht op bescherming van persoonsgegevens wordt omkaderd door een norm die niet alleen noodzakelijk is en in verhouding staat tot het nagestreefde doel, maar die ook voldoende duidelijk en nauwkeurig is en waarvan de toepassing voor de betrokken personen te voorzien is. Een gebrekkige voorzienbaarheid tast dus onvermijdelijk ook de wettelijkheid van de norm aan.

[...]

45. In de mate dat het ontwerp van samenwerkingsakkoord in een duidelijker opgave voorziet van de geviseerde categorieën van ontvangers, evenals de duidelijkere afbakening van de doeleinden (waarvoor deze derden de gegevens in kwestie kunnen aanwenden), kan een beraadslaging van het Informatieveiligheidscomité uiteraard een meerwaarde leveren op het vlak van het bijkomend preciseren van de uitvoeringsmodaliteiten, inzonderheid op het vlak van informatiebeveiliging.

De Autoriteit dringt er daarbij op aan dat - naast de functionele beschrijving van de informatiesystemen en van de informatiestromen die het voorwerp hebben uitgemaakt van een beraadslaging (zie artikel 5, laatste lid van het ontwerp van samenwerkingsakkoord) - ook de beraadslagingen van het Informatieveiligheidscomité zelf onverwijld en integraal worden gepubliceerd en voor een lange termijn raadpleegbaar worden gemaakt ».

B.27.3. De minister van Volksgezondheid heeft dienaangaande gepreciseerd dat « de taak van het Informatieveiligheidscomité [...] strikt afgebakend [is]. Het zal enkel kunnen beraadslagen voor gegevensmededelingen die gebeuren in het kader van dit samenwerkingsakkoord. In geen geval kan het Comité zelf andere doeleinden of andere categorieën van persoonsgegevens bepalen » (*Parl. St.*, Kamer, 2020-2021, DOC 55-1853/002, p. 13).

De Waalse minister van Gezondheid heeft ook gepreciseerd dat « enkel derden die belast zijn met een openbare opdracht en die wettelijk gemachtigd zijn om de persoonsgegevens te verwerken, de gegevens kunnen ontvangen » (*Parl. St.*, Waals Parlement, C.R.I, nr. 25, 2020-2021, 31 maart 2021, p. 73).

B.28. Wat de in de gegevensbank « Vaccinnet » vermelde persoonsgegevens betreft, bepaalt artikel 5 van het samenwerkingsakkoord twee categorieën van derden waaraan die gegevens kunnen worden meegedeeld : enerzijds, « personen of instanties die zijn belast met een taak van algemeen belang door of krachtens een wet, een decreet of een ordonnantie », waaraan, onder de in artikel 3, § 2, bedoelde gegevens, enkel de nodige gegevens gelet op de doeleinden van artikel 4, § 2, mogen worden meegedeeld en enkel indien die mededeling noodzakelijk is voor de uitvoering van de opdracht van algemeen belang van die personen of instanties; anderzijds, « onderzoeksinstellingen » indien de gegevens noodzakelijk zijn om wetenschappelijk of statistisch onderzoek te doen, na anonimisering of op zijn minst pseudonimisering voor het geval dat uitvoeren van de anonimisering wetenschappelijk of statistisch onderzoek niet mogelijk zou maken.

Bij artikel 5, derde lid, wordt de mededeling van die persoonsgegevens evenwel afhankelijk gesteld van een beraadslaging van de kamer « sociale zekerheid en gezondheid » van het Informatieveiligheidscomité, teneinde de naleving van de in dat artikel vermelde voorwaarden na te gaan.

B.29.1. Zoals in B.16.9 en B.16.10 is vermeld, waarborgt artikel 22 van de Grondwet, door aan de bevoegde wetgever de bevoegdheid voor te behouden om te bepalen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privé- en gezinsleven, aan elke burger dat geen inmenging in dat recht zal kunnen plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering.

Een delegatie aan een andere macht is niet in strijd met het wettigheidsbeginsel, voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever worden vastgesteld.

B.29.2. Artikel 6, lid 2, van de AVG bepaalt dat de lidstaten « specifiekere bepalingen » kunnen handhaven of invoeren ter aanpassing van de manier waarop de regels van de AVG worden toegepast met betrekking tot de verwerking die noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust (artikel 6, lid 1, c)) en de verwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen (artikel 6, lid 1, e)). Artikel 9, lid 2, h), van de AVG maakt de verwerking van gevoelige gegevens voor doeleinden van preventieve geneeskunde mogelijk, omringd met verschillende waarborgen, met name het beroepsgeheim. Artikel 9, lid 2, i), van de AVG bepaalt dat het Unierecht of lidstatelijk recht krachtens hetwelk de verwerking van gevoelige gegevens noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid, voorziet in « passende en specifieke maatregelen » ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim. Artikel 9, lid 4, bepaalt dat de lidstaten « bijkomende voorwaarden, waaronder beperkingen, » met betrekking tot onder meer de verwerking van gegevens over gezondheid kunnen handhaven of invoeren.

B.30.1. Het Informatieveiligheidscomité werd opgericht bij artikel 2, § 1, van de wet van 5 september 2018 « tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG » (hierna : de wet van 5 september 2018). In tegenstelling tot de sectorale comités die zijn afgeschaft bij de wet van 3 december 2017 « tot oprichting van de Gegevensbeschermingsautoriteit » die ze opvolgt en die waren opgenomen in de vroegere Commissie voor de bescherming van de persoonlijke levenssfeer, werd het Informatieveiligheidscomité opgericht als een nieuw onafhankelijk orgaan van de Gegevensbeschermingsautoriteit op grond van de voormelde artikelen 6, lid 2, en 9, lid 4, van de AVG (*Parl. St.*, Kamer, 2017-2018, DOC 54-3185/001, pp. 6-7 en 30; DOC 54-3185/005, pp. 7-10). Uit de parlementaire voorbereiding van de wet van 5 september 2018 blijkt dat de wetgever heeft gewild dat het Informatieveiligheidscomité noch als een verwerkingsverantwoordelijke, noch als een toezichthoudende autoriteit in de zin van de AVG werd beschouwd (*Parl. St.*, Kamer, 2017-2018, DOC 54-3185/001, pp. 8-10).

Overeenkomstig artikel 2, § 2, van de wet van 5 september 2018 bestaat het Informatieveiligheidscomité uit twee kamers : een kamer « sociale zekerheid en gezondheid » en een kamer « federale overheid ». De artikelen 2, § 1, en 4, § 1, eerste lid, van dezelfde wet bepalen dat de leden ervan voor een hernieuwbare termijn van zes jaar worden benoemd door de Kamer van volksvertegenwoordigers, die hen ook van hun opdracht kan ontheffen. Artikel 5 van dezelfde wet bepaalt dat de leden van het Informatieveiligheidscomité « van niemand onderrichtingen [krijgen] ». Uit de parlementaire voorbereiding blijkt dat de wetgever het Informatieveiligheidscomité heeft willen onttrekken aan elke hiërarchische controle (*Parl. St.*, Kamer, 2017-2018, DOC 54-3185/001, p. 10).

De bevoegdheid om administratieve beslissingen te nemen die wordt toevertrouwd aan de kamer « sociale zekerheid en gezondheid » van het Informatieveiligheidscomité bij artikel 5 van het samenwerkingsakkoord van 12 maart 2021 (de mededeling van persoonsgegevens toestaan of weigeren), is analoog aan die welke wordt toevertrouwd aan die kamer bij artikel 15, § 1, eerste lid, van de wet van 15 januari 1990 « houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid », vervangen bij artikel 18 van de wet van 5 september 2018, bij artikel 42, § 2, 3°, van de wet van 13 december 2006 « houdende diverse bepalingen betreffende gezondheid », zoals gewijzigd bij artikel 43 van de wet van 5 september 2018, en bij artikel 11 van de wet van 21 augustus 2008 « houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen », zoals gewijzigd bij artikel 50 van de wet van 5 september 2018. Die bepalingen machtigen de kamer « sociale zekerheid en gezondheid » van het Informatieveiligheidscomité om de mededeling toe te staan van, respectievelijk, (1) sociale gegevens van persoonlijke aard door de Kruispuntbank van de sociale zekerheid of door een instelling van sociale zekerheid aan een andere instelling van sociale zekerheid of aan een andere instantie dan een federale overheidsdienst, een programmatorische overheidsdienst of een federale instelling van openbaar nut, (2) persoonsgegevens die de gezondheid betreffen en (3) persoonsgegevens door of aan het eHealth-platform. Bij de uitoefening van hun toestemmingsbevoegdheid beperken de kamers van het Informatieveiligheidscomité zich ertoe na te gaan of de desbetreffende mededeling van persoonsgegevens de in de AVG omschreven beginselen van doelbinding, evenredigheid en veiligheid in acht neemt (*Parl. St.*, Kamer, 2017-2018, DOC 54-3185/001, pp. 6, 8 en 9).

Artikel 46, § 2, eerste lid, van de wet van 15 januari 1990 « houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid », vervangen bij artikel 39 van de wet van 5 september 2018, bepaalt dat de beraadslagingen van het Informatieveiligheidscomité « een algemene bindende draagwijdte tussen partijen en jegens derden » hebben. Volgens de parlementaire voorbereiding van de wet van 5 september 2018 hebben die beraadslagingen « een normatieve waarde (wet in materiële zin), overeenkomstig de grondwettelijke bepalingen en kunnen [zij] worden betwist volgens de geldende rechtsmiddelen indien ze tegenstrijdig zijn met hogere juridische normen » (*ibid.*, p. 8). Het tweede lid van dezelfde bepaling luidt :

« De Gegevensbeschermingsautoriteit kan elke beraadslaging van het informatieveiligheidscomité te allen tijde, ongeacht wanneer zij werd verleend, toetsen aan hogere rechtsnormen. Onverminderd haar andere bevoegdheden kan zij, als ze op een gemotiveerde wijze vaststelt dat een beraadslaging niet in overeenstemming is met een hogere rechtsnorm, het informatieveiligheidscomité vragen om die beraadslaging op de punten die ze aangeeft binnen de vijfenveertig dagen en uitsluitend voor de toekomst te heroverwegen. In voorkomend geval legt het informatieveiligheidscomité de gewijzigde beraadslaging ter advies voor aan de Gegevensbeschermingsautoriteit. Voor zover die niet binnen de vijfenveertig dagen bijkomende opmerkingen formuleert, wordt de gewijzigde beraadslaging geacht definitief te zijn ».

Artikel 46, § 1, 8°, van de wet van 15 januari 1990 « houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid », vervangen bij artikel 39 van de wet van 5 september 2018, bepaalt daarenboven dat het Informatieveiligheidscomité jaarlijks op de website van de Kruispuntbank en op de website van het eHealth-platform een beknopt verslag publiceert over de vervulling van zijn opdrachten tijdens het afgelopen jaar. In de parlementaire voorbereiding van de wet van 5 september 2018 wordt ten slotte vermeld dat tegen de beraadslagingen van het Informatieveiligheidscomité beroep kan worden ingesteld bij de Raad van State (*Parl. St.*, Kamer, 2017-2018, DOC 54-3185/001, pp. 10 en 31).

B.30.2. Uit het voorgaande blijkt dat, zoals het Hof bij zijn arrest nr. 110/2022 van 22 september 2022 (ECLI:BE:GHCC:2022:ARR.110) heeft geoordeeld, de beraadslagingen van het Informatieveiligheidscomité met name voor de personen wier verwerking van persoonsgegevens door dat Comité wordt toegestaan, een bindende draagwijdte hebben. Die beraadslagingen worden aan een zwakke controle van de Gegevensbeschermingsautoriteit onderworpen omdat die het Informatieveiligheidscomité enkel kan vragen om een beslissing die zij onwettig zou achten, te « heroverwegen » en advies te verlenen over de ingevolge die vraag gewijzigde beraadslaging. Hoewel aan de betrokken personen geen jurisdictioneel beroep tegen de beraadslagingen van het Informatieveiligheidscomité wordt ontzegd, wordt hun wel de waarborg ontnomen dat die aan parlementaire controle worden onderworpen. Noch de benoeming en de ontheffing van hun opdracht van de leden van het Informatieveiligheidscomité door de Kamer van volksvertegenwoordigers, noch de verplichting om jaarlijks het beknopt verslag over de vervulling van de opdrachten van het Informatieveiligheidscomité op de website van de Kruispuntbank en op de website van het eHealth-platform te publiceren, lijken immers op een dergelijke controle.

B.31. Zoals de afdeling wetgeving van de Raad van State heeft opgemerkt in haar advies over het voorontwerp van wet dat de wet van 2 april 2021 is geworden, is een dergelijke delegatie aan een instelling zoals het Informatieveiligheidscomité « in beginsel niet in overeenstemming met de algemene publiekrechtelijke beginselen omdat erdoor geraakt wordt aan het beginsel van de eenheid van de verordenende macht en een rechtstreekse parlementaire controle ontbreekt », in zoverre « de waarborgen [...] inzake de bekendmaking, de preventieve controle van de Raad van State, afdeling Wetgeving, en de duidelijke plaats in de hiërarchie der normen » ontbreken (*Parl. St.*, Kamer, 2020-2021, DOC 55-1853/001, p. 53). Dergelijke delegaties zouden enkel kunnen worden verantwoord voor zover zij zeer beperkt zouden zijn door hun detailmatige of hoofdzakelijk technische draagwijdte, hetgeen te dezen niet het geval is. De bepalingen, maatregelen en voorwaarden die de lidstaten krachtens artikel 6, lid 2, artikel 9, lid 2, i), en artikel 9, lid 4, van de AVG kunnen aannemen, doen niets af aan die vaststelling.

Door de kamer « sociale zekerheid en gezondheid » van het Informatieveiligheidscomité, waarvan het statuut niet wordt gepreciseerd in de wet, noch de beoordelingsbevoegdheid erbij wordt afgebakend, te machtigen tot het nemen van beslissingen inzake de verwerking van persoonsgegevens die voor derden bindend zijn, zonder dat dergelijke beslissingen aan parlementaire controle kunnen worden onderworpen, ontzegt artikel 5 van het samenwerkingsakkoord van 12 maart 2021 de betrokken personen de garantie van een dergelijke controle, zonder dat zulks te rechtvaardigen valt op grond van een vereiste die voortvloeit uit het recht van de Europese Unie.

B.32. Doordat het is gericht tegen de bestreden akten in zoverre daarbij instemming wordt verleend met artikel 5 van het samenwerkingsakkoord van 12 maart 2021, het eerste onderdeel van het enige middel, gegrond voor zover dat artikel betrekking heeft op de mededeling van de in artikel 3, § 2, van het voormelde samenwerkingsakkoord bedoelde gegevens die in de gegevensbank « Vaccinnet » zijn geregistreerd.

De bestreden akten moeten in die mate worden vernietigd in zoverre daarbij instemming wordt verleend met artikel 5 van het samenwerkingsakkoord van 12 maart 2021.

III. Wat betreft de bewaringstermijn van de in « Vaccinnet » geregistreerde gegevens, bedoeld in artikel 6, § 2 (tweede onderdeel)

B.33. In het tweede onderdeel van het middel is de verzoekende partij van mening dat de in artikel 6, § 2, van het samenwerkingsakkoord van 12 maart 2021 bedoelde bewaringstermijn van de in « Vaccinnet » geregistreerde gegevens onevenredig is, enerzijds, in zoverre de termijn van 30 jaar voor het bewaren van de gegevens vanaf de datum van vaccinatie tegen COVID-19 buitensporig zou zijn en, anderzijds, bij gebrek aan een maximumtermijn voor het bewaren van de gegevens.

B.34.1. Artikel 6, § 2, van het samenwerkingsakkoord van 12 maart 2021 bepaalt :

« De gegevens bedoeld in artikel 3, § 2, worden bewaard tot aan het overlijden van de persoon waaraan het vaccin tegen COVID-19 werd toegediend en minimum gedurende 30 jaar na de vaccinatie ».

B.34.2. Wat de in artikel 6 bedoelde bewaringstermijn van de gegevens betreft, wordt in de algemene toelichting bij het samenwerkingsakkoord van 12 maart 2021 vermeld :

« De gegevens m.b.t. de vaccinatiecodes worden bewaard tot 5 dagen na de dag van publicatie van het koninklijk besluit dat het einde van de toestand van de coronavirus COVID-19-epidemie afkondigt. Zolang de pandemie duurt is in dit kader immers een nauwgezette opvolging noodzakelijk.

Daarnaast regelt het artikel de bewaringstermijn van de persoonsgegevens van Vaccinnet tot aan het overlijden van de persoon waaraan het vaccin tegen COVID-19 werd toegediend en minimum gedurende 30 jaar na de vaccinatie.

Naast het belang voor de zorggebruiker en de zorgverleners om [te] allen tijde een juist beeld te hebben van de toegediende vaccinaties is deze bewaringstermijn vereist voor een correcte opvolging m.b.t. noodzakelijke hernieuwingen, zeker voor vaccins waarvan de duur van de bescherming vandaag nog niet bekend is. Algemeen worden persoonsgegevens die de gezondheid betreffen standaard minimum 30 jaar na het laatste contact bewaard in het medisch dossier. De bewaartermijn laat daarnaast een longitudinale opvolging voor wetenschappelijk onderzoek toe. Ten slotte is deze bewaartermijn van belang in het kader van de aansprakelijkheidsregels ten aanzien van betrokken actoren, gelet op de onzekerheid inzake de mogelijke ongewenste bijwerkingen op lange termijn.

Bedoeling is dat een vaccin liefst levenslang werkt. Daarom geeft men veel vaccins op jonge leeftijd en zijn er voor verschillende ziekten waartegen er gevaccineerd wordt achteraf geen nieuwe herhalingsvaccins nodig. Het is daarom wel van belang om ook na bv. 30 jaar nog te weten of iemand een bepaald vaccin gehad heeft. Het is belangrijk voor de arts maar ook voor de gevaccineerde om de vaccinatiestatus te kennen ook van reeds lang geleden geplaatste vaccins.

Anderzijds is het bij de wetenschappelijke opvolging van de werkzaamheid van vaccins ook nodig om zelfs na meer dan 30 jaar na te gaan of iemand gevaccineerd werd. Zo heeft men bijvoorbeeld gemerkt dat het vaccin tegen kinkhoest bij ouderen aan kracht verliest waardoor men een herhalingsvaccin plaatst. Om deze studies te doen moet men uiteraard weten of er vaccinatie was.

Ten laatste verschijnen de nevenwerkingen van geneesmiddelen waartoe vaccins behoren soms pas na vele jaren. Een klassiek voorbeeld van een geneesmiddel is diëthylstilbestrol (DES)[,] een hormoon dat aan vrouwen gegeven werd. Vele dochters geboren van de DES moeders bleken op volwassen leeftijd een verhoogd risico te hebben voor vagina- en baarmoederhalskanker. Indien men die data vernietigd zou hebben, had men misschien de link niet kunnen leggen. Maar laattijdige effecten kunnen ook positief zijn. Zo is er de hypothese dat mensen (bv. kinderen) die zelfs lang geleden een BCG vaccin tegen TBC kregen eventueel minder vatbaar zouden zijn voor COVID-19.

Ten slotte mag een beperkte set van gegevens gelinkt aan laboresultaten uit Gegevensbank I van het Samenwerkingsakkoord van 25 augustus 2020 niet gewist worden na 60 dagen. Deze gegevens zijn namelijk nodig voor de operationele processen en de doeleinden gelinkt aan de vaccinatieregistraties. Het gaat daarbij enerzijds om het doeleinde van geneesmiddelenbewaking. Voor dit doeleinde kan er in het kader van zogenaamde ' break through cases ', waarbij een gevaccineerde persoon alsnog COVID-19 krijgt, aan het betrokken labo gevraagd worden om een ' whole genome sequencing ' uit te voeren om de oorzaak van vaccin failure te kunnen onderzoeken. Daarnaast is de

bewaring van deze gegevens ook langer nodig voor het doeleinde van logistieke organisatie van de vaccinaties tegen COVID-19. Gegevens over voorgaande besmettingen, waarbij er reeds een zekere immuniteit aanwezig is, kunnen namelijk relevant zijn in de keuzes voor prioritisering van vaccinatie-doelgroepen » (*Belgisch Staatsblad* van 12 april 2021, pp. 32411-32412; zie ook *Parl. St.*, Kamer, 2020-2021, DOC 55-1853/001, pp. 16-18).

B.35.1. In haar advies over het voorontwerp van wet dat de wet van 2 april 2021 houdende instemming met het samenwerkingsakkoord van 12 maart 2021 is geworden, heeft de afdeling wetgeving van de Raad van State opgemerkt :

« 30. Overeenkomstig de Nederlandse tekst van artikel 6, § 2 van het samenwerkingsakkoord worden de gegevens uit de Vaccin[n]et-gegevensbank bewaard ' 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 '. Volgens de Franse tekst worden die gegevens bewaard ' 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 '. Volgens de Duitse tekst worden de gegevens bewaard ' *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* '.

Nog afgezien van de vraag of het verschillende voegwoord (' of ', ' et ' en ' und ') niet tot een verschillende draagwijdte leidt van die bepaling, vraagt de Raad van State zich af waarom wordt voorzien in een dergelijk lange termijn van dertig jaar, mede in het licht van artikel 5, lid 1, e), van de AVG.

Ook indien kan worden aangenomen dat de termijn van een jaar na het overlijden van de gevaccineerde persoon ingegeven is door overwegingen in verband met geneesmiddelenbewaking, wordt door de vermelding ' minstens ' geen maximale, maar een minimale bewaartermijn bepaald. Allicht schrijve men ' maximaal ' in plaats van ' minstens ' » (*ibid.*, pp. 54-55; zie ook *Parl. St.*, Vlaams Parlement, 2020-2021, nr. 708/1, p. 90; *Parl. St.*, Waals Parlement, 2020-2021, nr. 509/1, pp. 85-86; *Parl. St.*, Parlement van de Duitstalige Gemeenschap, 2020-2021, nr. 132/1, pp. 32-33; *Parl. St.*, Verenigde Vergadering van de Gemeenschappelijke Gemeenschapscommissie, 2020-2021, nr. B-65/1, pp. 18-19; *Parl. St.*, Vergadering van de Franse Gemeenschapscommissie, 2020-2021, nr. 45/1, pp. 33-34).

B.35.2. In haar advies nr. 16/2021 van 10 februari 2021 over het voorontwerp van samenwerkingsakkoord dat het samenwerkingsakkoord van 12 maart 2021 is geworden, heeft de Gegevensbeschermingsautoriteit opgemerkt :

« 51. De in toepassing van het ontwerp van samenwerkingsakkoord in Vaccinnet geregistreerde persoonsgegevens worden, in navolging van diens artikel 6, § 2, bewaard 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.

52. De Autoriteit is van oordeel dat de in het ontwerp van samenwerkingsakkoord voorziene bewaartermijn van 30 jaar gebeurlijk kan worden weerhouden voor gepseudonimiseerde gegevens in het kader van eerder wetenschappelijke/statistische doeleinden. Voor meer operationele doeleinden komt deze uitermate lange bewaartermijn overmatig voor ».

B.35.3. Wat de bewaringstermijn van de gegevens betreft, heeft de Waalse minister van Gezondheid eraan herinnerd dat « de geldigheidsduur van het vaccin thans nog niet bekend is » en dat « het belangrijk is om de vaccinatiestatus van een persoon te kennen, ook vele jaren na de vaccinatie » (*Parl. St.*, Waals Parlement, C.R.I., nr. 25, 2020-2021, 31 maart 2021, p. 74).

B.35.4. Voor de Vergadering van de Franse Gemeenschapscommissie heeft de minister van Gezondheid eveneens gepreciseerd :

« Wat betreft de gegevensbank Vaccinnet+, bedraagt de bewaringstermijn van de gegevens 30 jaar omdat die duur reeds bestond vóór het samenwerkingsakkoord. Dat lijkt lang maar werd door wetenschappers noodzakelijk bevonden. Het is immers uiterst belangrijk dat de gevaccineerde persoon en de zorgverleners zich een beeld kunnen vormen van de vaccinaties die tijdens het leven van die persoon werden toegediend.

Dat kan ook nuttig zijn in het kader van herhalingsvaccins. De duur van de bescherming van het vaccin tegen COVID-19 is nog niet bekend. Het is onmogelijk om vandaag te weten wat er zal gebeuren over zes maanden, een jaar, of zelfs twee jaar. Het is dus belangrijk om op dat ogenblik de gelegenheid te hebben om de vaccinatiedossiers van de burgers te raadplegen teneinde exact te weten welke vaccins zij hebben gekregen, binnen welke termijnen, enz.

Voor de studies met betrekking tot de wetenschappelijke opvolging van de werkzaamheid van de vaccins is het ook nodig om na meer dan 30 jaar na te gaan of een burger werd gevaccineerd. Als voorbeeld haalt hij het vaccin tegen kinkhoest aan, dat bij ouderen aan kracht verliest en een herhaling vereist.

Die bewaringstermijn is dus belangrijk, in het kader van de aansprakelijkheidsregels ten aanzien van de betrokken actoren. Gezien de onzekerheid inzake de mogelijke ongewenste bijwerkingen op lange termijn, hoewel die zeldzaam zijn, en zelfs uiterst zeldzaam, is het dan ook uiterst belangrijk om vele jaren na het toedienen van een vaccin anamneses te kunnen uitvoeren » (*Parl. St.*, Vergadering van de Franse Gemeenschapscommissie, 2020-2021, nr. 45/2, p. 12).

B.36.1. Overeenkomstig het beginsel van opslagbeperking van de gegevens moeten persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is (artikel 5, lid 1, punt e), van de AVG).

B.36.2. Artikel 6, § 2, van het samenwerkingsakkoord van 12 maart 2021 voorziet in een maximumtermijn voor het bewaren van de gegevens.

De in de gegevensbank « Vaccinnet » geregistreerde gegevens worden minstens 30 jaar en maximaal tot de datum van het overlijden van de betrokken persoon bewaard.

B.37.1. De noodzaak van de bewaringstermijn van de gegevens wordt beoordeeld ten aanzien van de voorliggende omstandigheden, en rekening houdend met het feit dat de algemeen aanvaarde termijn voor het bewaren van gezondheidsdossiers en in het kader van wetenschappelijk onderzoek met betrekking tot gezondheid vrij lang is.

B.37.2. Krachtens artikel 9, § 1, van de wet van 22 augustus 2002 betreffende de rechten van de patiënt heeft de patiënt « ten opzichte van de beroepsbeoefenaar recht op een zorgvuldig bijgehouden en veilig bewaard patiëntendossier » en, op zijn verzoek, « voegt de beroepsbeoefenaar door de patiënt verstrekte documenten toe aan het hem betreffende patiëntendossier ».

In de parlementaire voorbereiding van die bepaling wordt vermeld :

« In het eerste lid van artikel 9, § 1, wordt aan de patiënt het recht toegekend op een zorgvuldig bijgehouden en veilig bewaard patiëntendossier. De normen waaraan het patiëntendossier moet voldoen, [onder meer] op inhoudelijk vlak, worden niet in dit ontwerp geregeld. Hiervoor kan [onder meer] worden verwezen naar het K.B. van 3 mei 1999 betreffende het algemeen medisch dossier en het K.B. van 3 mei 1999 houdende bepaling van de algemene minimumvoorwaarden waaraan het medisch dossier, bedoeld in artikel 15 van de wet op de ziekenhuizen[,] dient te voldoen » (*Parl. St.*, Kamer, 2001-2002, DOC 50-1642/001, p. 29).

In artikel 1 van het koninklijk besluit van 3 mei 1999 « betreffende het Algemeen Medisch Dossier » wordt het « Algemeen Medisch Dossier » (AMD) omschreven als « een functionele en selectieve verzameling van relevante medische, sociale en administratieve gegevens m.b.t. een patiënt, die het voorwerp uitmaken van een manuele of geïnformatiseerde verwerking », en dat met name « ziektegeschiedenis en antecedenten (doorgestane ziekten, operaties, vaccinatiestatus) » omvat.

Artikel 1, § 3, van het koninklijk besluit van 3 mei 1999 « houdende bepaling van de algemene minimumvoorwaarden [waaraan] het medisch dossier, bedoeld in artikel 15 van de wet op de ziekenhuizen, gecoördineerd op 7 augustus 1987, moet voldoen », bepaalt dat het medisch dossier dat voor elke patiënt in een ziekenhuis wordt aangelegd, « gedurende minstens dertig jaar in het ziekenhuis bewaard [dient] te worden ».

Artikel 35 van de wet van 22 april 2019 « inzake de kwaliteitsvolle praktijkvoering in de gezondheidszorg » bepaalt :

« De gezondheidszorgbeoefenaar bewaart het patiëntendossier gedurende minimum 30 jaar en maximum 50 jaar te rekenen vanaf het laatste patiëntencontact ».

Artikel 24 van de Code van medische deontologie bepaalt :

« De arts bewaart de patiëntendossiers veilig en met inachtneming van het beroepsgeheim gedurende dertig jaar na het laatste contact met de patiënt. Daarna mag hij die patiëntendossiers vernietigen.

De arts die zijn praktijk stopzet, bezorgt de arts die de patiënt aanwijst, of de patiënt alle nuttige inlichtingen voor de continuïteit van de zorg ».

Uit het voorgaande vloeit voort dat een bewaringstermijn van minstens 30 jaar de gewoonlijk aanvaarde termijn inzake gegevens over gezondheid vormt.

B.37.3. Er dient eveneens rekening te worden gehouden met de pandemische noodomstandigheden die de totstandkoming, de vergunning voor het in de handel brengen, de productie en de toediening van de vaccins tegen COVID-19 omringen en met de noodzaak om, op middellange en lange termijn, de doeltreffendheid van die vaccins en de eventuele ongewenste bijwerkingen ervan te kunnen beoordelen. Het is met name met het oog op die beoordeling dat de doeleinden met betrekking tot het verstrekken van gezondheidszorg en behandelingen (artikel 4, § 2, 1°), de geneesmiddelenbewaking van de vaccins (artikel 4, § 2, 2°), de monitoring en surveillance na vergunning van de vaccins (artikel 4, § 2, 8°) of het uitvoeren van wetenschappelijke of statistische studies (artikel 4, § 2, 10°) werden bepaald.

B.37.4. Gelet op het voorgaande, gaat de bewaring van de vaccinatiegegevens tegen COVID-19 tot aan het overlijden van de gevaccineerde persoon niet verder dan wat noodzakelijk is ten aanzien van de doeleinden waarvoor zij worden verwerkt.

B.38. Doordat het is gericht tegen de bestreden akten in zoverre daarbij instemming wordt verleend met artikel 6, § 2, van het samenwerkingsakkoord, is het tweede onderdeel van het enige middel, niet gegrond.

IV. Wat betreft de ontstentenis van een voorafgaande effectbeoordeling, vereist bij artikel 35 van de AVG (tweede onderdeel)

B.39. De verzoekende partij bekritiseert het niet uitvoeren van een voorafgaande gegevensbeschermingseffectbeoordeling in de zin van artikel 35 van de AVG, zodat de in het middel bedoelde bepalingen, bij gebrek aan die effectbeoordeling, zouden zijn geschonden.

B.40. In de algemene toelichting bij het samenwerkingsakkoord van 12 maart 2021 wordt vermeld :

« Het samenwerkingsakkoord werd voor advies voorgelegd aan de Gegevensbeschermingsautoriteit (advies 16-2021 van 10 februari 2021), de ' Vlaamse Toezichtscommissie ' (advies 2021/13 van 17 februari 2021), de adviezen van de Raad van State (68.832/VR, 68836/VR, 68837/VR[,] 68.839/VR, 68.840/VR, 68/844/VR van 18 februari 2021), de Vlaamse Raad WVG (advies van 16 februari 2021), het inter-Franstalig overlegorgaan en het overleg in het intra-Franstalige ministerieel comité voor overleg (advies van 15 februari 2021).

Een gegevensbeschermingseffectenbeoordeling wordt opgesteld met toepassing van de artikelen 35 en 36 van de Algemene Verordening Gegevensbescherming » (*Belgisch Staatsblad* van 12 april 2021, p. 32398).

B.41.1. In haar advies over het voorontwerp van wet dat de wet van 2 april 2021 houdende instemming met het samenwerkingsakkoord van 12 maart 2021 is geworden, heeft de afdeling wetgeving van de Raad van State opgemerkt :

« Op de vraag of die effectbeoordeling reeds werd uitgevoerd, antwoordden de gemachtigden het volgende :

' Nee, dit zal nog gebeuren. '

De steller van het voorontwerp dient er bijgevolg op toe te zien dat die effectbeoordeling naar behoren wordt uitgevoerd, zo mogelijk voordat de wetgevende vergadering instemt met het voorliggende samenwerkingsakkoord » (*Parl. St.*, Kamer, 2020-2021, DOC 55-1853/001, p. 46; zie ook *Parl. St.*, Vlaams Parlement, 2020-2021, nr. 708/1, p. 82; *Parl. St.*, Waals Parlement, 2020-2021, nr. 509/1, pp. 81-82; *Parl. St.*, Parlement van de Duitstalige Gemeenschap, 2020-2021, nr. 132/1, pp. 27-28; *Parl. St.*, Verenigde Vergadering van de Gemeenschappelijke Gemeenschapscommissie, 2020-2021, nr. B-65/1, pp. 11-12; *Parl. St.*, Vergadering van de Franse Gemeenschapscommissie, 2020-2021, nr. 45/1, p. 29).

B.41.2. In haar advies nr. 16/2021 van 10 februari 2021 heeft de Gegevensbeschermingsautoriteit opgemerkt, zoals zij dat reeds had gedaan in haar advies nr. 138/2020 van 18 december 2020 met betrekking tot het koninklijk besluit van 24 december 2020 (punt 21) :

« Aangezien de in het ontwerp van samenwerkingsakkoord omkaderde gegevensregistraties inzake COVID-19-vaccinaties, gepaard gaan met een grootschalige verwerking van een bijzondere categorie van persoonsgegevens, nl. gegevens over gezondheid, is(/zijn) de verwerkingsverantwoordelijke(n), krachtens artikel 35.3 van de AVG verplicht om vóór de verwerking een gegevensbeschermingseffectbeoordeling uit te voeren. Hoewel de Autoriteit reeds op het belang van deze bepaling wees in haar advies nr. 138/2020, geeft de aanvrager in het formulier voor het aanvragen van een advies nog steeds aan dat de met het ontwerp van samenwerkingsakkoord beoogde verwerkingen niet werden onderworpen aan dergelijke gegevensbeschermingseffectbeoordeling. De Autoriteit dringt hierop ook in onderhavig advies nogmaals aan » (punt 19).

B.41.3. In het verslag van 23 maart 2021 heeft de minister van Volksgezondheid aangegeven :

« De gegevensbeschermingseffectbeoordeling (*data protection impact assessment*) is uitgevoerd en een samenvatting is beschikbaar » (*Parl. St.*, Kamer, 2020-2021, DOC 55-1853/002, p. 14).

B.42. Indien de verwerking van persoonsgegevens waarschijnlijk een « hoog risico » inhoudt « voor de rechten en vrijheden van natuurlijke personen », moet de verwerkingsverantwoordelijke, overeenkomstig artikel 35 van de AVG, vóór de verwerking een beoordeling uitvoeren van het effect van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens. Krachtens artikel 36 van de AVG moet de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit raadplegen, wanneer uit de effectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken.

B.43. Bij artikel 35 van de AVG wordt het uitvoeren van een gegevensbeschermingseffectbeoordeling opgelegd vóór de materiële handeling van de verwerking die een hoog risico kan inhouden voor de rechten en vrijheden van natuurlijke personen, maar wordt die niet opgelegd vóór of bij de totstandkoming van een wetsbepaling met betrekking tot een dergelijke verwerking. Aangezien het voorafgaande karakter van de effectbeoordeling een materiële handeling van de verwerking betreft, behoort het niet tot de bevoegdheid van het Hof maar wel tot de bevoegdheid van de justitiële of administratieve rechter.

Die vaststelling doet geen afbreuk aan de verplichting voor de lidstaten om « de toezichthoudende autoriteit [te raadplegen] bij het opstellen van een voorstel voor een door een nationaal parlement vast te stellen wetgevingsmaatregel, of een daarop gebaseerde regelgevingsmaatregel in verband met verwerking », overeenkomstig artikel 36, lid 4, van de AVG, verplichting waaraan de wetgever te dezen heeft voldaan.

B.44.1. Ten slotte is de kritiek die is gericht tegen de vertrouwelijkheid van de effectbeoordeling, die door de verzoekende partij is opgeworpen in haar memorie van antwoord, niet ontvankelijk, omdat zij erop neerkomt dat de draagwijdte van het tweede onderdeel van het middel wordt gewijzigd, dat zich beperkte tot het bekritiseren van de ontstentenis van een voorafgaande effectbeoordeling.

Het staat immers niet aan een verzoekende partij in haar memorie van antwoord het middel, zoals door haarzelf omschreven in het verzoekschrift, te wijzigen. Een bezwaar dat, zoals te dezen, in een memorie van antwoord wordt aangebracht maar dat verschilt van datgene dat in het verzoekschrift is geformuleerd, is dan ook een nieuw middel en is onontvankelijk.

B.44.2. Voor het overige legt de AVG niet de verplichting op om die beoordeling te publiceren (Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking « waarschijnlijk een hoog risico inhoudt » in de zin van Verordening 2016/679, 4 april 2017, laatstelijk gewijzigd op 4 oktober 2017, Groep gegevensbescherming artikel 29, p. 22). De vertrouwelijkheid kan immers worden verantwoord door het feit dat de effectbeoordeling betrekking heeft op eventuele veiligheidsrisico's, en met name op de technische beschrijving van de geplande maatregelen om die risico's te beperken. Die analyse openbaar maken zou de beveiliging van de verwerking van die gegevens bijgevolg in gevaar kunnen brengen, en zou dan ook het recht op eerbiediging van het privéleven en de bescherming van persoonsgegevens in gevaar kunnen brengen.

B.45. Doordat het is gericht tegen de bestreden akten in zoverre zij niet zouden zijn voorafgegaan door een voorafgaande effectbeoordeling, is het tweede onderdeel van het enige middel, niet gegrond.

V. Wat betreft de terugwerkende kracht van de gevolgen van het samenwerkingsakkoord tot 24 december 2020, bedoeld in artikel 12 (derde onderdeel)

B.46. In het derde onderdeel van het middel is de verzoekende partij van mening dat de bestreden akten in strijd zijn met het beginsel van de niet-retroactiviteit van de wetten dat vereist dat de inhoud van het recht voorzienbaar en toegankelijk is, zodat de rechtzoekende in redelijke mate de gevolgen van een bepaalde handeling kan voorzien op het tijdstip dat die handeling wordt verricht.

Aldus bepaalt artikel 12 van het samenwerkingsakkoord van 12 maart 2021 dat de bepalingen van dat akkoord terugwerkende kracht hebben tot de dag van de inwerkingtreding van het koninklijk besluit van 24 december 2020, terwijl het in artikel 4, § 2, van het samenwerkingsakkoord vermelde elfde doeleinde, zo beklemtoont de verzoekende partij, niet voorkwam in het koninklijk besluit van 24 december 2020.

B.47.1. Artikel 12 van het samenwerkingsakkoord van 12 maart 2021 bepaalt :

« Dit samenwerkingsakkoord heeft uitwerking met ingang van 24 december 2020 voor wat betreft de bepalingen die inhoudelijk overeenstemmen met het koninklijk besluit van 24 december 2020 betreffende de registratie en de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 en met ingang van 11 februari 2021 voor wat betreft de andere bepalingen.

Dit samenwerkingsakkoord heeft uitwerking tot de herziening of de herroeping ervan nadat de Centrale Secretarie van het Overlegcomité het schriftelijk akkoord heeft ontvangen van alle partijen om een einde te stellen aan het samenwerkingsakkoord en na de bekendmaking van een bericht in het *Belgisch Staatsblad* met de bevestiging van dit schriftelijk akkoord ».

B.47.2. In de algemene toelichting bij het samenwerkingsakkoord van 12 maart 2021 wordt vermeld :

« Artikel 12 regelt de uitwerking in de tijd van het samenwerkingsakkoord en voorziet in de mogelijkheid van de herziening of de opheffing ervan » (*Belgisch Staatsblad* van 12 april 2021, p. 32413; zie ook *Parl. St.*, Kamer, 2020-2021, DOC 55-1853/001, p. 19).

B.48. In haar advies over het voorontwerp van wet dat de bestreden wet van 2 april 2021 houdende instemming met het samenwerkingsakkoord van 12 maart 2021 is geworden, heeft de afdeling wetgeving van de Raad van State opgemerkt :

« Overeenkomstig artikel 12 van het samenwerkingsakkoord heeft het uitwerking met ingang van 24 december 2020.

De niet-retroactiviteit van regels op het hiërarchische niveau van een wetgevende norm is een waarborg ter voorkoming van rechtsonzekerheid. Die waarborg vereist dat de inhoud van het recht voorzienbaar en toegankelijk is, zodat de rechtzoekende in redelijke mate de gevolgen van een bepaalde handeling kan voorzien op het tijdstip dat die handeling wordt verricht. De terugwerkende kracht kan enkel worden verantwoord wanneer ze onontbeerlijk is voor de verwezenlijking van een doelstelling van algemeen belang.

In dit geval wordt met de terugwerkende kracht een doelstelling van algemeen belang nagestreefd, namelijk het in stand houden van een voldoende rechtszeker juridisch kader voor de strijd tegen de COVID-19-pandemie.

Zoals reeds werd uiteengezet in de adviezen over de instemmingsteksten met het samenwerkingsakkoord over de contactopsporing kan in de gegeven omstandigheden uitzonderlijk terugwerkende kracht worden verleend aan de bepalingen van het samenwerkingsakkoord die inhoudelijk overeenstemmen met hetgeen is geregeld in de federale regelgeving die dringend inspeelt op noodwendigheden van de bestrijding van de COVID-19-pandemie, met ingang van de datum van inwerkingtreding van die federale regelgeving, meer bepaald het koninklijk besluit van 24 december 2020 ' betreffende de registratie en de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 '.

Die verantwoording geldt echter niet voor nieuwe elementen die niet overeenstemmen met de verwerking van persoonsgegevens zoals die in de feiten heeft plaatsgevonden sinds die datum. Er moet dan ook op worden toegezien dat de regeling in dit samenwerkingsakkoord volledig aansluit bij die feitelijke uitwerking » (*Parl. St.*, Kamer, 2020-2021, DOC 55-1853/001, pp. 56-57; zie ook *Parl. St.*, Vlaams Parlement, 2020-2021, nr. 708/1, p. 92; *Parl. St.*, Waals Parlement, 2020-2021, nr. 509/1, pp. 86-87; *Parl. St.*, Parlement van de Duitstalige Gemeenschap, 2020-2021, nr. 132/1, pp. 34-35; *Parl. St.*, Verenigde Vergadering van de Gemeenschappelijke Gemeenschapscommissie, 2020-2021, nr. B-65/1, pp. 20-21; *Parl. St.*, Vergadering van de Franse Gemeenschapscommissie, 2020-2021, nr. 45/1, p. 35).

B.49.1. In de in B.2 in herinnering gebrachte context moet worden beklemtoond dat het samenwerkingsakkoord van 12 maart 2021 werd gesloten binnen een termijn van minder dan drie maanden, gelijktijdig met de start van de vaccinatiecampagne in januari 2021 in omstandigheden van dringende noodzakelijkheid, teneinde de COVID-19-pandemie te bestrijden.

Bij het koninklijk besluit van 24 december 2020, dat is genomen overeenkomstig artikel 11 van de wet van 22 december 2020, alsook bij het protocolakkoord van 27 januari 2021 hebben de verschillende overheden van het land de rechtsgrond aangenomen die de registratie van de vaccinatiegegevens mogelijk maakt, in afwachting van een samenwerkingsakkoord.

B.49.2. Zoals in B.4 is vermeld, wordt in de inhoud van het samenwerkingsakkoord de inhoud overgenomen van het protocolakkoord van 27 januari 2021 dat zelf de inhoud van het koninklijk besluit van 24 december 2020 overnam, met enkele aanpassingen. De datum van opheffing van het koninklijk besluit van 24 december 2020, alsook die van het protocolakkoord van 27 januari 2021, worden vastgesteld op de datum waarop het samenwerkingsakkoord van 12 maart 2021 uitwerking heeft.

Uit het voorgaande vloeit voort dat de in artikel 12 van het samenwerkingsakkoord van 12 maart 2021 vervatte terugwerkende kracht wordt verantwoord door het doel van algemeen belang dat erin bestaat de rechtszekerheid te garanderen door de wettelijke basis van de registratie van de vaccinatiegegevens in « Vaccinnet » te consolideren en te vervangen. Zoals de afdeling wetgeving van de Raad van State heeft beklemtoond, wordt met die terugwerkende kracht « een doelstelling van algemeen belang nagestreefd, namelijk het in stand houden van een voldoende rechtszeker juridisch kader voor de strijd tegen de COVID-19-pandemie » (*Parl. St.*, Kamer, 2020-2021, DOC 55-1853/001, p. 56).

B.49.3. Die terugwerkende kracht heeft daarenboven geen onevenredige gevolgen. Door te bepalen dat het samenwerkingsakkoord van 12 maart 2021 uitwerking heeft met ingang van 24 december 2020 voor wat betreft de bepalingen die inhoudelijk overeenstemmen met het koninklijk besluit van 24 december 2020 « betreffende de registratie en de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 » en met ingang van 11 februari 2021 voor wat betreft de andere bepalingen, doet artikel 12 van het samenwerkingsakkoord van 12 maart 2021 immers geen afbreuk aan de rechtszekerheid en aan de legitieme verwachtingen, aangezien het geen wijziging van de inhoud van de voorheen bestaande regeling met zich meebrengt, maar zich ertoe beperkt die te consolideren.

Er moet immers worden vastgesteld dat het samenwerkingsakkoord, voor de elementen die overeenstemmen met de verwerking van persoonsgegevens zoals erin was voorzien bij het koninklijk besluit van 24 december 2020, uitwerking heeft op de datum van inwerkingtreding van dat koninklijk besluit, terwijl het samenwerkingsakkoord, voor de nieuwe elementen die niet overeenstemmen met de verwerking van persoonsgegevens zoals die in de feiten concreet heeft plaatsgevonden sedert die datum, uitwerking heeft op de datum van inwerkingtreding van het protocolakkoord van 27 januari 2021, zijnde op 11 februari 2021. In dat verband moet worden vastgesteld dat het in artikel 4, § 2, 11°, van het samenwerkingsakkoord van 12 maart 2021 bedoelde doeleinde, dat de verzoekende partij bekritiseert, reeds in het protocolakkoord van 27 januari 2021 was vervat.

B.50. Doordat het is gericht tegen de bestreden akten in zoverre daarbij instemming wordt verleend met artikel 12 van het samenwerkingsakkoord van 12 maart 2021, is het derde onderdeel van het enige middel, niet gegrond.

Wat betreft het verzoek tot handhaving van de gevolgen

B.51. De institutionele partijen verzoeken om de gevolgen van de bestreden akten te handhaven in geval van vernietiging.

B.52.1. Wanneer een beroep tot vernietiging, gericht tegen een wetskrachtige norm, gegrond is, heeft het Hof, krachtens artikel 8, eerste lid, van de bijzondere wet van 6 januari 1989, enkel de bevoegdheid om de betrokken akte geheel of gedeeltelijk te vernietigen.

Wanneer het, zoals te dezen het geval is, een wetskrachtige norm vernietigt, kan het Hof, krachtens artikel 8, derde lid, van de bijzondere wet, de gevolgen van een vernietigde bepaling voorlopig handhaven tot de wetgever een einde heeft gesteld aan de vastgestelde ongrondwettigheid, en voor de termijn die het bepaalt.

B.52.2. Uit de rechtspraak van het Hof van Justitie blijkt dat de beginselen van de voorrang en van de volle werking van het recht van de Europese Unie zich verzetten tegen een voorlopige handhaving van nationale maatregelen die in strijd zijn met het rechtstreeks toepasselijke Unierecht (HvJ, grote kamer, 8 september 2010, C-409/06, *Winner Wetten GmbH*). Op grond van die rechtspraak vermag het Grondwettelijk Hof dus geen gevolg te verlenen aan een verzoek tot handhaving van de gevolgen van een vernietigde wetgevende akte, doordat afbreuk zou worden gedaan aan de volle werking van het Unierecht.

B.52.3. Voor het overige bestaat er geen aanleiding om dat verzoek in te willigen, rekening houdend met de beperkte draagwijdte van de uitgesproken vernietiging.

Om die redenen,

het Hof

- vernietigt de wet van 2 april 2021, het decreet van de Vlaamse Gemeenschap van 2 april 2021, het decreet van de Duitstalige Gemeenschap van 29 maart 2021, de ordonnantie van de Gemeenschappelijke Gemeenschapscommissie van 2 april 2021, het decreet van het Waalse Gewest van 1 april 2021 en het decreet van de Franse Gemeenschapscommissie van 1 april 2021 « houdende instemming met het samenwerkingsakkoord van 12 maart 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19 », in zoverre daarbij instemming wordt verleend met artikel 5 van het samenwerkingsakkoord van 12 maart 2021, voor zover dat artikel betrekking heeft op de mededeling van de in artikel 3, § 2, van het voormelde samenwerkingsakkoord bedoelde gegevens die in de gegevensbank « Vaccinnet » zijn geregistreerd;

- verwerpt het beroep voor het overige.

Aldus gewezen in het Frans, het Nederlands en het Duits, overeenkomstig artikel 65 van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, op 1 juni 2023.

De griffier, De voorzitter,

F. Meersschaut P. Nihoul

VERFASSUNGSGERICHTSHOF

[C − 2023/42867]

Auszug aus dem Entscheid Nr. 84/2023 vom 1. Juni 2023

Geschäftsverzeichnisnummer 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. Meersschaut, 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).

(...)

II. *Rechtliche Würdigung*

(...)

In Bezug auf die angefochtenen Akte und ihren Kontext

B.1. Die klagende Partei beantragt die 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 » (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.*, Verenigte 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 abstimmte 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 Arsenals 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 föderierten 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 Impfzertifikats, 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-Impfzertifikaten eingeleitet oder verfolgen entsprechende Pläne. Diese Impfzertifikate 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 Impfzertifikate 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 Impfzertifikat festgelegt werden. Mit diesem Impfzertifikat 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 Impfzertifikat 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 Impfzertifikate 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 « Impfzertifikat » bestimmt:

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

(2) Das Impfzertifikat 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 Impfzertifikat 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 Impfzertifikats 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 Impfzertifikat 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 Impfzertifikate 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 Impfzertifikate 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 Impfzertifikate für einen in Unterabsatz 2 genannten COVID-19-Impfstoff an, so erkennen sie zu gleichen Bedingungen auch Impfzertifikate 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 Impfzertifikat 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 Impfserie und Gesamtzahl der Dosen in der Impfserie;

″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 neue 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 92*bis* 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 Nichtigerklärung 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 Nichtigerklärung 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 Nichtigerklärung 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 Nichtigerklärung 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 Nichtigerklärung offensichtlich unzulässig ist.

B.8.4. Die Klage auf Nichtigerklärung, 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 Impfcode eine Einladung zur Impfung gegen COVID-19 gemäß der von den zuständigen Behörden festgelegten Impfstrategie erhalten. Dieser Impfcode 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 Impflicht 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 Impfzertifikats 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, *Vavřička 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 Pflegeerbringern 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 bestimmbare 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 der 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 Menschenmit 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 derWeltgesundheitsorganisation 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.*, Verenigte 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 Impfzertifikate 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 staatssicherheitlichen 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 Impfrate 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 unterstreich, 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 DatenschutzGrundverordnung 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.*, Verenigte 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 desselben Bestimmung lautet:

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

Artikel 46 § 1 Nr. 8 des Gesetzes vom 15. Januar 1990 « über die Errichtung und Organisation einer Zentralen Datenbank der sozialen Sicherheit », ersetzt durch Artikel 39 des Gesetzes vom 5. September 2018, bestimmt außerdem, dass der Informationssicherheitsausschuss jährlich auf der Website der Zentralen Datenbank und auf der Website der eHealth-Plattform einen kurzen Bericht über die Erfüllung 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 seinem Entscheid 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 Zusammenarbeitsabkommens 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 Impfcode 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 BCGTuberkulose-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 Impfversagens 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 Vaccinet 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.*, Verenigte 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.*, Verenigte 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 Regelungsmaßnahmen, 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 Erwiderungsschriftsatz 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 Erwiderungsschriftsatz den Klagegrund zu ändern, den sie selbst in der Klageschrift verfasst hat. Ein Beschwerdegrund, der wie im vorliegenden Fall in einem Erwiderungsschriftsatz 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 Rechtsunterworfene 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.*, Verenigte 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 Nichtigerklärung.

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 — F. Meersschaut

Der Präsident — P. Nihoul

MINISTERE DE LA DEFENSE

[C − 2023/47868]

21 NOVEMBRE 2023. — Loi modifiant la loi du 11 avril 2003 instituant un service volontaire d'utilité collective (1)

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

La Chambre des représentants à adopté et Nous sanctionnons ce qui suit:

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

MINISTERIE VAN LANDSVERDEDIGING

[C − 2023/47868]

21 NOVEMBER 2023.— Wet tot wijziging van de wet van 11 april 2003 tot instelling van een vrijwillige dienst van collectief nut (1)

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

De Kamer van volksvertegenwoordigers heeft aangenomen en Wij bekrachtigen hetgeen volgt :

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.