



RAAD VAN STATE
afdeling Wetgeving

CONSEIL D'ÉTAT
section de législation

advies 67.719/VR
van 15 juli 2020

avis 67.719/VR
du 15 juillet 2020

over

sur

een voorontwerp van wet 'houdende instemming met het Samenwerkingsakkoord 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 regionale overheden 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, afgesloten te Brussel op 2 juli 2020 en tot intrekking van het koninklijk besluit nr. 18 van 2 mei 2020, het koninklijk besluit nr. 25 van 28 mei 2020 en het koninklijk besluit nr. 44 van 26 juni 2020 inzake een databank bij Sciensano in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19'

un avant-projet de loi 'portant assentiment à l'Accord de coopération entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano, conclu à Bruxelles le 2 juillet 2020 et retirant l'arrêté royal n° 18 du 4 mai 2020, l'arrêté royal n° 25 du 28 mai 2020 et l'arrêté royal n° 44 du 26 juin 2020 concernant une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19'

Op 3 juli 2020 is de Raad van State, afdeling Wetgeving, door de Minister van Volksgezondheid verzocht binnen een termijn van vijf werkdagen, verlengd tot acht werkdagen^(*), een advies te verstrekken over een voorontwerp van wet 'houdende instemming met het Samenwerkingsakkoord 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 regionale overheden 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, afgesloten te Brussel op 2 juli 2020 en tot intrekking van het koninklijk besluit nr. 18 van 2 mei 2020, het koninklijk besluit nr. 25 van 28 mei 2020 en het koninklijk besluit nr. 44 van 26 juni 2020 inzake een databank bij Sciensano in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19'.

Het voorontwerp is door de verenigde kamers onderzocht op 10 juli 2020. De verenigde kamers waren samengesteld uit Jo BAERT, kamervoorzitter, voorzitter, Martine BAGUET, kamervoorzitter, Jeroen VAN NIEUWENHOVE, Luc CAMBIER, Bernard BLERO en Koen MUYLLE, staatsraden, Jan VELAERS en Sébastien VAN DROOGHENBROECK, assessoren, en Annemie GOOSSENS, griffier, en Charles-Henri VAN HOVE, toegevoegd griffier.

Het verslag is uitgebracht door Cedric JENART en Anne-Stéphanie RENSON, adjunct-auditeurs.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Martine BAGUET, kamervoorzitter, en Jeroen VAN NIEUWENHOVE, staatsraad.

Het advies, waarvan de tekst hierna volgt, is gegeven op 15 juli 2020.

*

^(*) Deze verlenging vloeit voort uit artikel 84, § 1, eerste lid, 3°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, waarin wordt bepaald dat de termijn van vijf werkdagen verlengd wordt tot acht werkdagen in het geval waarin het advies gegeven wordt door de verenigde kamers met toepassing van artikel 85*bis*.

Le 3 juillet 2020, le Conseil d'État, section de législation, a été invité par la Ministre de la Santé publique à communiquer un avis, dans un délai de cinq jours ouvrables, prorogé à huit jours ouvrables (**), sur un avant-projet de loi 'portant assentiment à l'Accord de coopération entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts des personnes (présümées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano, conclu à Bruxelles le 2 juillet 2020 et retirant l'arrêté royal n° 18 du 4 mai 2020, l'arrêté royal n° 25 du 28 mai 2020 et l'arrêté royal n° 44 du 26 juin 2020 concernant une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19'.

L'avant-projet a été examiné par les chambres réunies le 10 juillet 2020. Les chambres réunies étaient composées de Jo BAERT, président de chambre, président, Martine BAGUET, président de chambre, Jeroen VAN NIEUWENHOVE, Luc CAMBIER, Bernard BLERO et Koen MUYLLE, conseillers d'État, Jan VELAERS et Sébastien VAN DROOGHENBROECK, assesseurs, et Annemie GOOSSENS, greffier, et Charles-Henri VAN HOVE, greffier assumé.

Le rapport a été présenté par Cedric JENART et Anne-Stéphanie RENSON, auditeurs adjoints.

La concordance entre la version française et la version néerlandaise de l'avis a été vérifiée sous le contrôle de Martine BAGUET, président de chambre, et Jeroen VAN NIEUWENHOVE, conseiller d'État.

L'avis, dont le texte suit, a été donné le 15 juillet 2020.

*

(**) Cette prorogation résulte de l'article 84, § 1^{er}, alinéa 1^{er}, 3^o, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, qui dispose que le délai de cinq jours ouvrables est prorogé à huit jours ouvrables dans le cas où l'avis est donné par les chambres réunies en application de l'article 85*bis*.

1. Volgens artikel 84, § 1, eerste lid, 2°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, moeten in de adviesaanvraag de redenen worden opgegeven tot staving van het spoedeisende karakter ervan.

In het onderhavige geval wordt het verzoek om spoedbehandeling gemotiveerd als volgt:

“Het verzoek om spoedbehandeling is gemotiveerd door de omstandigheid dat dit voorontwerp betrekking heeft op een buitengewone crisissituatie, namelijk de gevolgen van de COVID-19-pandemie die momenteel in België heerst, wat bijzondere en ernstige problemen oplevert in termen van de volksgezondheid;

Dat het van vitaal belang is voor de volksgezondheid en voor het vermijden van een heropflakking van de COVID-19 pandemie, dat een gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams kan plaatsvinden met het oog op een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn, op basis van een gegevensbank bij Sciensano;

Dat de afdeling wetgeving in haar advies 67.425/3 over een wetsvoorstel ‘tot oprichting van een databank bij Sciensano in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19’ (Parl.St. Kamer 2019-20, nr. 55-1249/001) oordeelde dat de materie die het voorwerp uitmaakt van voornoemd wetsvoorstel, alsook van dit voorontwerp betrekking heeft zowel op federale als op gemeenschapsbevoegdheden, en de beoogde regelgeving enkel doorgang kan vinden indien ze zou worden omgevormd tot een samenwerkingsakkoord waarvoor parlementaire instemming is vereist;

Dat momenteel het bijzondere volmachtenbesluit nr. 44 van 26 juni 2020 omwille van de dringende noodzakelijkheid voorziet in een voorlopige regelgeving m.b.t. deze materie, in afwachting van een meer duurzame en rechtszekere oplossing onder de vorm van een samenwerkingsakkoord;

Dat het koninklijk besluit nr. 44 ophoudt uitwerking te hebben op 15 oktober 2020;

Dat het voor de goede werking, de continuïteit en het vertrouwen van de burger in het systeem van het contactonderzoek van belang is dat omtrent de beoogde gegevensverwerking zo snel mogelijk de nodig juridische zekerheid wordt gecreëerd;

Dat het bijgevolg van belang is dat dit samenwerkingsakkoord zo snel mogelijk en tegelijkertijd met de verschillende instemmingsakten gepubliceerd wordt in het Belgisch Staatsblad.”

*

2. Aangezien de adviesaanvraag is ingediend op grond van artikel 84, § 1, eerste lid, 3°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving haar onderzoek tot de rechtsgrond¹ voor het voorontwerp, de bevoegdheid van de steller van de handeling, alsmede tot de vraag of aan de te vervullen vormvereisten is voldaan, overeenkomstig artikel 84, § 3, van de voormelde gecoördineerde wetten.

Met betrekking tot die drie punten zijn de volgende opmerkingen te maken over het voorontwerp.

*

VOORGESCHIEDENIS EN STREKKING VAN HET VOORONTWERP VAN WET EN VAN HET SAMENWERKINGSAKKOORD

3. Het koninklijk besluit nr. 18 van 4 mei 2020 ‘tot oprichting van een databank bij Sciensano in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19’ voorzag in de oprichting van een databank bij Sciensano² in het kader van de strijd tegen de verspreiding van COVID-19, teneinde gegevens in te zamelen van personen die zijn getest op COVID-19 of met een bevestigde diagnose van COVID-19, personen waarvan een vermoeden bestaat van besmetting en personen waarmee de voormelde personen in contact zijn geweest. De geldingsduur van dit besluit tot 4 juni 2020, werd verlengd tot 30 juni 2020 bij het koninklijk besluit nr. 25 van 28 mei 2020 ‘tot wijziging van het koninklijk besluit nr. 18 van 4 mei 2020 tot oprichting van een databank bij Sciensano in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19’. Daarop volgde het koninklijk besluit nr. 44 van 26 juni 2020 ‘betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden 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’, dat de regeling in het koninklijk besluit nr. 18 van 4 mei 2020 inhoudelijk ongewijzigd overnam en dat nog steeds geldig is.³ Geen van deze besluiten werd om advies voorgelegd aan de afdeling Wetgeving van de Raad van State.

De inhoud van het koninklijk besluit nr. 18 van 4 mei 2020 werd bijna integraal overgenomen in een wetsvoorstel ‘tot oprichting van een databank bij Sciensano in het kader van

¹ Aangezien het om een voorontwerp van wet gaat, wordt onder “rechtsgrond” de overeenstemming met de hogere rechtsnormen verstaan.

² Sciensano is een openbare instelling met rechtspersoonlijkheid die onder meer een aantal opdrachten inzake gezondheid en inzake het ondersteunen van het gezondheidsbeleid vervult (zie de artikelen 3 en 4 van de wet van 25 februari 2018 ‘tot oprichting van Sciensano’).

³ Overeenkomstig artikel 17 ervan “houdt [het besluit] op uitwerking te hebben op de dag waarop een samenwerkingsakkoord 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 regionale overheden 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 in werking treedt” en uiterlijk op 15 oktober 2020.

de strijd tegen de verspreiding van het coronavirus COVID 19⁴, dat samen met een aantal amendementen erop⁵ om advies werd voorgelegd aan de Raad van State. In advies 67.425/3-67.426/3-67.427/3 van 26 mei 2020⁶ stelde de Raad van State vast dat de in het voorstel geregelde databank, de ermee gepaard gaande verwerking van persoonsgegevens, alsook de bepalingen met betrekking tot de opdrachten en de werkwijze van het contactcentrum betrekking hebben op de opsporing en de voorkoming van besmettingen met COVID-19. Het wetsvoorstel heeft dan ook grotendeels betrekking op de bevoegdheid van de gemeenschappen voor de opsporing en de strijd tegen de besmettelijke en de sociale ziekten als een onderdeel van hun bevoegdheden inzake preventieve gezondheidszorg,⁷ zodat de Raad van State adviseerde om het wetsvoorstel om te vormen tot een samenwerkingsakkoord waarvoor de parlementaire instemming is vereist. Die conclusie werd herhaald in advies 67.482/3 van 3 juni 2020⁸ over een ander amendement⁹ op hetzelfde wetsvoorstel.

4. Samen met het voormelde wetsvoorstel werd aan de Raad van State ook een wetsvoorstel ‘betreffende het gebruik van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking’¹⁰ om advies voorgelegd. Op 26 mei 2020 heeft de Raad van State daarover advies 67.424/3¹¹ gegeven, waarin hij vaststelde dat de in het voorstel geregelde digitale contactopsporingsapplicaties en de ermee gepaard gaande verwerking van persoonsgegevens betrekking hebben op de opsporing en de voorkoming van besmettingen met COVID-19. Het wetsvoorstel heeft dan ook grotendeels betrekking op de bevoegdheid van de gemeenschappen voor de opsporing en de strijd tegen de besmettelijke en de sociale ziekten als een onderdeel van hun bevoegdheden inzake preventieve gezondheidszorg. Ook in dit geval adviseerde de Raad van State om het wetsvoorstel om te vormen tot een samenwerkingsakkoord waarvoor de parlementaire instemming is vereist.

5. Het thans om advies voorgelegde voorontwerp van wet beoogt de instemming met een samenwerkingsakkoord dat een grondige herwerking bevat van de regeling die vervat is in de twee voormelde wetsvoorstellen. De partijen bij dit samenwerkingsakkoord zijn de federale overheid, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie.

⁴ *Parl.St.* Kamer 2019-20, nr. 55-1249/001.

⁵ *Ibid.*, nrs. 55-1249/002 en 55-1249/003.

⁶ *Ibid.*, nr. 55-1249/006.

⁷ Artikel 5, § 1, I, eerste lid, 8°, van de bijzondere wet van 8 augustus 1980 ‘tot hervorming der instellingen’. Zie ook *Parl.St.* Senaat 1979-80, nr. 434/2, 125 en *Parl.St.* Kamer 1979-80, nr. 627/10, 52. Deze bevoegdheid werd impliciet bevestigd in adv.RvS 34.339/AV van 29 april 2003 over een voorontwerp dat heeft geleid tot het decreet van de Vlaamse Gemeenschap en het Vlaamse Gewest van 21 november 2003 ‘betreffende het preventieve gezondheidsbeleid’, *Parl.St.* VI.Parl. 2002-03, nr. 1709/1, 147-155, alsook uitdrukkelijk in adv.RvS 38.381/3 van 7 juli 2005 over een ontwerp van koninklijk besluit ‘tot vaststelling van de profylactische maatregelen en de verplichte aangifte aan de cel medische bewaking van pathologieën van epidemische aard’ en in adv.RvS 53.018/VR van 13 mei 2013 over een ontwerp van koninklijk besluit ‘houdende de gezondheidscontrole van het internationale verkeer’.

⁸ *Parl.St.* Kamer 2019-20, nr. 55-1249/009.

⁹ *Ibid.*, nr. 55-1249/004.

¹⁰ *Parl.St.* Kamer 2019-20, nr. 55-1251/001.

¹¹ *Ibid.*, nr. 55-1251/003.

5.1. Bij het samenwerkingsakkoord worden bij Sciensano vier gegevensbanken opgericht (Gegevensbanken I, III, IV en V), naast de bestaande gegevensbank, die nader wordt geregeld in het licht van de strijd tegen COVID-19 (Gegevensbank II). Deze vijf gegevensbanken worden bij artikel 1, § 1, 5° tot 9°, van het samenwerkingsakkoord omschreven.

– Gegevensbank I is de algemene, centrale gegevensbank bij Sciensano voor de verwerking en uitwisseling van gegevens voor de verwerkingsdoeleinden bepaald in het samenwerkingsakkoord. Deze centrale databank voorziet in de uitwisseling van gegevens met de gegevensbanken die worden opgericht ter ondersteuning van de contactcentra van de gemeenschappen.

– Gegevensbank II is de bestaande gegevensbank bij Sciensano die is opgericht ter uitvoering van een samenwerkingsovereenkomst met het Rijksinstituut voor ziekte- en invaliditeitsverzekering (hierna: RIZIV) met het oog op het verhogen van de epidemiologische, klinische en andere kennis.¹² De gegevens, verstrekt in het kader van het manuele contactonderzoek moeten onderzoekinstellingen, met inbegrip van Sciensano, in staat stellen wetenschappelijke of statistische studies uit te voeren in verband met de verspreiding van het coronavirus COVID-19 en om het beleid in de strijd tegen het coronavirus te ondersteunen, middels de uitwisseling van de gegevens met de Gegevensbank I.

– Gegevensbank III is de gegevensbank met belorders en orders voor de medewerkers van het contactcentrum.

– Gegevensbank IV is de gegevensbank met contactgegevens van collectiviteiten.

– Gegevensbank V is de centrale loglijst die toelaat om de werking van de digitale contactopsporingsapplicatie op een gecontroleerde manier te laten verlopen en die bij Sciensano afzonderlijk van Gegevensbank I en II wordt gehouden. Een digitale contactopsporingsapplicatie op basis van DP3T¹³ bestaat immers uit een mobiele applicatie die door de gebruiker vrijwillige lokaal op diens toestel geïnstalleerd en gebruikt kan worden, en een centrale loglijst die in Gegevensbank V bewaard wordt.

5.2. Hoofdstuk I van het samenwerkingsakkoord bevat algemene bepalingen. Artikel 1 bevat een aantal definities (paragraaf 1), vermeldt de doelstellingen van het samenwerkingsakkoord (paragraaf 2), bepaalt dat geen afbreuk wordt gedaan aan de regelgeving van de bevoegde overheden inzake contactonderzoek voor het opsporen van besmettelijke ziekten (paragraaf 3), schrijft voor dat de partijen de maatregelen moeten nemen om het samenwerkingsakkoord uit te voeren en om hun bestaande initiatieven ermee in overeenstemming te brengen (paragraaf 4), voorziet in de mogelijkheid van uitvoerende samenwerkingsakkoorden (paragraaf 5) en bepaalt dat de gezondheidszorgverleners en de gecontacteerde personen ontheven zijn van hun beroepsgeheim (paragraaf 6). Artikel 2 richt Gegevensbank I op (paragraaf 1), kadert Gegevensbank II binnen dit samenwerkingsakkoord

¹² Zie artikel 22, 20°, van de wet 'betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen', gecoördineerd op 14 juli 1994, toegevoegd bij de wet van 10 april 2014.

¹³ DP3T is de afkorting van het open protocol "Decentralised Privacy-Preserving Proximity Tracing" (zie https://en.wikipedia.org/wiki/Decentralized_Privacy-Preserving_Proximity_Tracing).

(paragraaf 2), stelt de Gegevensbanken III en IV in (paragraaf 3), wijst Sciensano aan als verwerkingsverantwoordelijke van de Gegevensbanken I en II (paragraaf 4) en bepaalt dat de deelstaten de verwerkingsverantwoordelijken voor de Gegevensbanken III en IV zullen aanwijzen (paragraaf 5).

Hoofdstuk II omvat artikel 3, dat de verwerkingsdoeleinden regelt met betrekking tot de terbeschikkingstelling van persoonsgegevens door Gegevensbank I (paragraaf 1), alsook met betrekking tot de verwerking van persoonsgegevens door de bevoegde overheden of de bevoegde agentschappen (paragraaf 2) en door de mobiele teams en de gezondheidsinspectiediensten van de gemeenschappen (paragraaf 3). Er wordt voorzien in een algemeen verbod om persoonsgegevens te verwerken voor andere doelstellingen (paragraaf 4).

Hoofdstuk III omvat artikel 4, dat de categorieën van personen omschrijft wiens persoonsgegevens worden verwerkt in het kader van dit samenwerkingsakkoord. Die categorieën worden bepaald in artikel 1, § 1, 12° tot 17°.

– Personen Categorie I: de personen voor wie de arts een COVID-19-test heeft voorgeschreven;

– Personen Categorie II: de personen bij wie een COVID-19-test is uitgevoerd;

– Personen Categorie III: de personen bij wie de arts een ernstig vermoeden heeft dat ze besmet zijn, zonder dat een COVID-19-test is uitgevoerd of voorgeschreven of waarbij de COVID-19-test uitwees dat ze niet besmet waren;

– Personen Categorie IV: de personen met wie hetzij (i) de Personen Categorie II voor zover de COVID-19-test uitwees dat ze besmet zijn, hetzij (ii) de Personen Categorie III in contact zijn geweest gedurende een periode van veertien dagen voor en na de eerste tekenen van de besmetting;

– Personen Categorie V: de behandelende artsen van de Personen Categorieën I, II, en III;

– Personen Categorie VI: de referentiearts of – bij gebrek aan een referentiearts bij de betrokken collectiviteit – de administratief verantwoordelijke van collectiviteiten waarmee de Personen Categorieën I, II en III gedurende een periode van veertien dagen voor en veertien dagen na de eerste symptomen van de besmetting in contact is geweest.

Hoofdstuk IV bepaalt de categorieën van persoonsgegevens die verwerkt worden in het kader van het samenwerkingsakkoord. Artikel 5 schrijft voor dat de gegevensverwerking moet gebeuren overeenkomstig de AVG¹⁴ en de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’. Artikel 6 schrijft voor dat de verplichte meldingen op grond van gemeenschapsregelgeving gebeurt aan Gegevensbank I (paragraaf 1) en omschrijft de categorieën van persoonsgegevens die

¹⁴ 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)’.

in die gegevensbank worden verwerkt voor respectievelijk de Personen Categorie I, de Personen Categorie II, de Personen Categorie III en de Personen Categorie IV (paragrafen 2 tot 5). De paragrafen 6 en 7 omschrijven bijkomende te verwerken persoonsgegevens voor bepaalde categorieën personen en clusters, die worden verzameld of aangeleverd door de bevoegde mobiele teams of de gezondheidsinspectiediensten. Artikel 7 omschrijft de categorieën van persoonsgegevens die verwerkt worden in Gegevensbank III, namelijk de persoonsgegevens die worden meegedeeld door Sciensano vanuit Gegevensbank I aan de contactcentra (paragraaf 1), de persoonsgegevens voor Gegevensbank III met betrekking tot de Personen Categorie II die na een COVID-19-test besmet bleken te zijn, en de Personen Categorie III (paragraaf 2), de Personen Categorie IV (paragraaf 3) en de Personen Categorie VI (paragraaf 4). Artikel 8 omschrijft de categorieën van persoonsgegevens die verwerkt worden in Gegevensbank IV met betrekking tot de Personen Categorie V en Categorie VI. Artikel 9 omschrijft de categorieën van persoonsgegevens die na pseudonimisering verwerkt worden in Gegevensbank II met betrekking tot de Personen Categorie I, Categorie II en Categorie III (paragraaf 1) en de Personen Categorie IV (paragraaf 2).

Hoofdstuk V omvat artikel 10 dat de toegang regelt tot persoonsgegevens door de contactcentra (paragraaf 1) en door de mobiele teams en de gezondheidsinspectiediensten (paragraaf 2) en dat de doorgifte van persoonsgegevens na pseudonimisering regelt van Gegevensbank I naar Gegevensbank II (paragraaf 3).

Hoofdstuk VI betreft de bevoegdheid van het informatieveiligheidscomité¹⁵. Artikel 11 regelt de voorafgaande beraadslaging in dat comité in bepaalde gevallen (paragrafen 1 en 2) en de verduidelijkende bevoegdheid van dat comité (paragraaf 3). Er wordt ook voorzien in de nadere regeling van bepaalde aspecten van het samenwerkingsakkoord in een uitvoerend samenwerkingsakkoord (paragraaf 4). Artikel 12 bepaalt de nadere regels die het informatieveiligheidscomité kan vaststellen (paragraaf 1) en regelt de toegang tot het Rijksregister en de registers van de Kruispuntbank van de sociale zekerheid (paragraaf 2), alsook de voorafgaande beraadslaging in het informatieveiligheidscomité voor de mededeling van persoonsgegevens uit andere authentieke bronnen dan Gegevensbank I (paragraaf 3).

Hoofdstuk VII omvat artikel 13, dat betrekking heeft op de veiligheidsmaatregelen die Sciensano moet nemen om een op het risico afgestemd beveiligingsniveau te waarborgen.

Hoofdstuk VIII heeft betrekking op de digitale contactopsporingsapplicaties. Artikel 14 beschrijft de doelstelling van digitale contactopsporingsapplicaties (paragraaf 1) en regelt de beperkingen inzake de verwerking van persoonsgegevens door middel van die applicaties (paragraaf 2), alsook de minimale voorwaarden voor die applicaties (paragraaf 3). De applicaties moeten de principes vervat in artikel 5 van de AVG respecteren (paragraaf 4) en moeten gebaseerd zijn op vrijwillige basis (paragraaf 5). De bewaartermijn van de gegevens met betrekking tot contacten wordt geregeld (paragraaf 6), alsook de doelstellingen van de gegevensverwerking (paragraaf 7). Er moet een gegevensbeschermingseffectenbeoordeling

¹⁵ Oppericht bij 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'.

worden opgesteld en gepubliceerd (paragraaf 8). Er wordt ook voorzien in de nadere regeling van bepaalde aspecten van de digitale contactopsporingsapplicaties in een uitvoerend samenwerkingsakkoord (paragraaf 9).

Hoofdstuk IX omvat artikel 15, dat de maximale bewaringstermijn regelt van persoonsgegevens voor de Gegevensbanken I, III, IV en V (paragraaf 1) en II (paragraaf 2).

Hoofdstuk X betreft de transparantie en de rechten van betrokken personen. Artikel 16 verplicht Sciensano om als verwerkingsverantwoordelijke passende maatregelen te nemen inzake de communicatie van de rechten van de betrokken personen (paragraaf 1), om een website te creëren en te onderhouden (paragraaf 2), om een systeem te onderhouden en te beheren voor de uitoefening van door de AVG bepaalde rechten (paragraaf 3) en om een overeenkomst te sluiten met de bevoegde overheden en hun agentschappen met betrekking tot hun verantwoordelijkheden inzake de uitoefening van de rechten van de betrokken personen en het verstrekken van informatie (paragraaf 4).

Hoofdstuk VIII (lees XI) bevat verscheidene slotbepalingen. Artikel 17 regelt de beslechting van geschillen tussen de partijen door een samenwerkingsgerecht. Artikel 18 draagt de Interministeriële Conferentie Volksgezondheid op om toezicht te houden op de uitvoering en naleving van de bepalingen van het samenwerkingsakkoord en om aanpassingen voor te stellen. Artikel 19 regelt de uitwerking in de tijd van het samenwerkingsakkoord (paragraaf 1) en voorziet in de mogelijkheid van de beëindiging ervan door een nieuw samenwerkingsakkoord (paragraaf 2).

BEVOEGDHEID

6. Zoals reeds is uiteengezet in de opmerkingen 3 en 4, werd in de adviezen 67.425/3-67.426/3-67.427/3 en 67.424/3 geconcludeerd tot het sluiten van een samenwerkingsakkoord tussen de federale overheid en de gemeenschappen voor de beoogde regelingen inzake de verwerking van persoonsgegevens met betrekking tot de manuele en de digitale contactopsporing. Ook al is het samenwerkingsakkoord waarmee de instemming wordt beoogd, een grondige inhoudelijke herwerking van de twee wetsvoorstellen waarover die adviezen zijn uitgebracht, toch is de bevoegdheidsconclusie dezelfde, onder voorbehoud van wat volgt.

6.1. Bij het bijzonder decreet van 3 april 2014 en de decreten van 4 en 11 april 2014 ‘relatif aux compétences de la Communauté française dont l’exercice est transféré à la Région wallonne et à la Commission communautaire française’, hebben respectievelijk de Franse Gemeenschap, de Franse Gemeenschapscommissie en het Waalse Gewest overeenkomstig artikel 138 van de Grondwet in onderlinge overeenstemming beslist dat onder meer de bevoegdheid van de Franse Gemeenschap inzake het gezondheidsbeleid, bedoeld in artikel 5, § 1, I, van de bijzondere wet van 8 augustus 1980 ‘tot hervorming der instellingen’ wordt uitgeoefend door het Waalse Gewest en de Franse Gemeenschapscommissie, waaronder ook de gemeenschapsbevoegdheid inzake zorginstellingen, met inbegrip van ziekenhuizen (met uitzondering van de universitaire ziekenhuizen) en inzake preventieve gezondheidszorg (onder meer met uitzondering “des activités et services de médecine préventive destinés aux nourrissons,

aux enfants, aux élèves et aux étudiants” en “de ce qui relève des missions confiées à l’Office de la Naissance et de l’Enfance (ONE)”.¹⁶

In zoverre de regeling in het samenwerkingsakkoord ook verplichtingen inhoudt voor zorginstellingen, waaronder ziekenhuizen,¹⁷ moeten naast de huidige partijen bij het samenwerkingsakkoord ook de Franse Gemeenschap en de Franse Gemeenschapscommissie als partijen bij het samenwerkingsakkoord worden betrokken.

De Franse Gemeenschap heeft immers de uitoefening behouden van haar principiële bevoegdheid inzake het opleggen van verplichtingen aan universitaire ziekenhuizen in het Franse taalgebied en aan de universitaire ziekenhuizen in het tweetalige gebied Brussel-Hoofdstad die wegens hun organisatie beschouwd moeten worden uitsluitend te behoren tot de Franse Gemeenschap.¹⁸

De Franse Gemeenschapscommissie oefent, van haar kant, de principiële bevoegdheid uit inzake het opleggen van verplichtingen aan privéziekenhuizen in het tweetalige gebied Brussel-Hoofdstad die wegens hun organisatie beschouwd moeten worden uitsluitend te behoren tot de Franse Gemeenschap.¹⁹

De gemachtigden²⁰ verklaarden in dat verband het volgende:

“[T]ijdens verschillende [interkabinettenwerkgroepen] heeft de Franse Gemeenschapscommissie zelf aangegeven dit deel van hun bevoegdheid door middel van de Gemeenschappelijke Gemeenschapscommissie te willen regelen. Hierdoor is de Franse Gemeenschapscommissie uiteindelijk geen partij meer bij het samenwerkingsakkoord, maar wordt zij vertegenwoordigd door de Gemeenschappelijke Gemeenschapscommissie.”

Bevoegdheidsregels zijn dwingende rechtsregels van openbare orde die zich niet lenen tot mechanismen als afstand of vertegenwoordiging door onderlinge instemming tussen overheden. De conclusie is dan ook dat zowel de Franse Gemeenschap als de Franse Gemeenschapscommissie aangezocht moeten worden als partij bij het samenwerkingsakkoord. Indien dit leidt tot inhoudelijke aanpassingen van de regeling in het samenwerkingsakkoord, zullen de voorontwerpen van instemmingsteksten met het aangepaste samenwerkingsakkoord opnieuw om advies aan de Raad van State moeten worden voorgelegd.

6.2. Zowel in het opschrift als in het dispositief van het samenwerkingsakkoord wordt systematisch verwezen naar de “regionale overheden”. Met de uitdrukking “regionale overheden” kan evenwel niet naar behoren worden verwezen naar de gemeenschapsoverheden die partij zijn (of dienen te zijn) bij het samenwerkingsakkoord. Het woord “regionale” dient dan ook uit het opschrift en uit het dispositief van het samenwerkingsakkoord te worden weggelaten.

¹⁶ Artikel 3, 6°, van de voormelde decreten.

¹⁷ Zie de artikelen 2, § 1, en 6, § 3, tweede lid, van het samenwerkingsakkoord.

¹⁸ Zie artikel 128, § 2, van de Grondwet, alsook artikel 3, 6°, van de voormelde decreten.

¹⁹ Zie artikel 128, § 2, van de Grondwet, alsook artikel 3, 6°, van de voormelde decreten.

²⁰ Hiermee (en bij de volgende vermeldingen ervan) worden de gemachtigden bedoeld die zijn aangewezen in de adviesaanvraag over het voorontwerp van instemmingswet, dat heeft geleid tot advies 67.719/VR.

VORMVEREISTEN

7.1. Artikel 14 van het samenwerkingsakkoord, dat betrekking heeft op de digitale contactopsporingsapplicaties, bevat een aantal technische voorschriften in de zin van artikel 1, lid 1, f), van richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 ‘betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij’, meer bepaald als regels betreffende diensten van de informatiemaatschappij in de zin van artikel 1, lid 1, e), van die richtlijn.

Dergelijke technische voorschriften moeten overeenkomstig artikel 5 van richtlijn (EU) 2015/1535 worden aangemeld bij de Europese Commissie. In dat geval geldt een wachtperiode van (minstens) drie maanden vooraleer het wetsvoorstel kan worden aangenomen, overeenkomstig artikel 6 van de richtlijn. Die wachtperiode geldt evenwel niet, overeenkomstig artikel 6, lid 7, als een lidstaat om dringende redenen wegens een ernstige en onvoorziene situatie die verband houdt met de bescherming van (onder meer) de gezondheid van mensen, op zeer korte termijn technische voorschriften moet uitwerken en deze onmiddellijk daarop moet vaststellen en invoeren, zonder dat raadpleging mogelijk is. In dat geval is de mededeling aan de Commissie nog steeds vereist; in de mededeling moet de reden voor de urgentie worden vermeld. De Commissie spreekt zich dan zo spoedig mogelijk uit over de mededeling.

Bijgevolg moet het samenwerkingsakkoord worden aangemeld bij de Europese Commissie, waarbij dan de urgentie van de goedkeuring ervan kan worden uiteengezet ter verantwoording van het niet in acht nemen van de voorgeschreven wachttermijn.²¹

7.2. Daarnaast rijst de vraag of het voormelde artikel 14 van het samenwerkingsakkoord onder het toepassingsgebied valt van de dienstenrichtlijn.²² Het ter beschikking stellen van een digitale contactopsporingsapplicatie moet worden beschouwd als een dienst, waarvan het mogelijk is dat die tegen een vergoeding wordt aangeboden, of die vergoeding nu afkomstig is van de overheid of - eventueel via reclame-inkomsten - van de gebruiker. Het samenwerkingsakkoord waarborgt alleszins niet dat de applicaties worden aangeboden als een niet-economische dienst van algemeen belang.²³ De uitzondering voor de diensten van de gezondheidszorg²⁴ kan ook niet worden ingeroepen, omdat de applicaties geen betrekking hebben op activiteiten die in de lidstaat waar de dienst wordt verricht, zijn voorbehouden aan beoefenaren van gereguleerde beroepen in de gezondheidszorg.²⁵

Het is dan ook mogelijk dat de dienstenrichtlijn toepasselijk is,²⁶ zodat de voormelde bepaling van het samenwerkingsakkoord moet worden getoetst aan de artikelen 14

²¹ Zie in dezelfde zin adv.RvS 67.424/3, opmerking 10.

²² Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 ‘betreffende diensten op de interne markt’.

²³ Zie artikel 2, lid 2, a), van de dienstenrichtlijn.

²⁴ Zie artikel 2, lid 2, f), van de dienstenrichtlijn.

²⁵ *Handboek voor de implementatie van de Dienstenrichtlijn*, Europese Commissie, 2007, p. 12. Zie ook overweging 22 bij de dienstenrichtlijn.

²⁶ De uitzonderingsgronden in artikel 2, lid 2, c) en i), lijken alleszins ook niet toepasselijk in dit geval.

en 15 ervan met betrekking tot de eisen die worden gesteld aan de uitoefening van een dienstenactiviteit op het grondgebied van België.²⁷ Op het eerste gezicht lijkt het samenwerkingsakkoord geen verboden eisen als bedoeld bij artikel 14 te bevatten, evenmin als niet-discriminerende eisen als bedoeld bij artikel 15, lid 2. De Raad van State beschikt evenwel niet over het vereiste technische inzicht in de specifieke eisen ten aanzien van de digitale contactopsporingsapplicaties om daarover een sluitend oordeel te kunnen vellen. In voorkomend geval zou toch nog een aanmelding bij de Europese Commissie overeenkomstig artikel 15, lid 7, van de dienstenrichtlijn vereist kunnen zijn.²⁸

ONDERZOEK VAN HET SAMENWERKINGSAKKOORD

ALGEMENE OPMERKINGEN

A. Authentieke Duitse versie van het samenwerkingsakkoord

8. Er blijkt nog geen authentieke Duitse versie van het samenwerkingsakkoord te bestaan die door alle partijen is ondertekend. Volgens de verklaringen van de gemachtigden was die versie nog in voorbereiding bij de indiening van de adviesaanvraag. Aangezien de Nederlandse en de Franse authentieke versie van het samenwerkingsakkoord werden ondertekend door -onder meer- de minister-president en de bevoegde minister van de Duitstalige Gemeenschap en gelet op de spoedeisendheid van de regeling in het samenwerkingsakkoord kan de Raad van State uitzonderlijk aanvaarden dat het ontbreken van de authentieke Duitse versie van het samenwerkingsakkoord de ontvankelijkheid van de adviesaanvraag niet in het gedrang brengt.

B. Verenigbaarheid met de hogere regelgeving inzake de bescherming van persoonsgegevens

9. Het voorliggende samenwerkingsakkoord heeft het over de verwerkingen van persoonsgegevens die een inmenging vormt in het recht op eerbiediging van het privéleven van de betrokkenen, dat inzonderheid wordt gewaarborgd bij artikel 22 van de Grondwet en bij artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM).

Om in het licht van de voornoemde bepalingen aanvaardbaar te zijn, moet de inmenging in het recht op eerbiediging van het privéleven worden geformuleerd in duidelijke en voldoende nauwkeurige bewoordingen die het mogelijk maken de hypothesen te voorzien waarin de wetgever een dergelijke inmenging toestaat. Elke inmenging in het recht op eerbiediging van

²⁷ Er wordt immers niet voorzien in een vergunningsstelsel, zodat niet moet worden getoetst aan de artikelen 9 tot 13 van de dienstenrichtlijn.

²⁸ Zie in dezelfde zin adv.RvS 67.424/3, opmerking 11.

het privéleven moet bovendien steunen op een redelijke verantwoording en evenredig zijn met de door de wetgever nagestreefde doelstellingen.²⁹

Hoewel de inmengingen waarin het voorliggende samenwerkingsakkoord voorziet een legitiem doel nastreven, namelijk de bescherming van de gezondheid en de bescherming van de rechten en vrijheden van anderen,³⁰ dient te worden nagegaan of aan de vereisten van wettelijkheid, relevantie en evenredigheid wordt voldaan, zowel wat de manuele als de digitale contactopsporing betreft die bij het samenwerkingsakkoord geregeld worden.

1. Het legaliteitsbeginsel vervat in artikel 22 van de Grondwet.

10.1. Krachtens artikel 22 van de Grondwet geldt voor elke verwerking van persoonsgegevens en, meer in het algemeen, voor elke schending van het recht op het privéleven, dat het legaliteitsbeginsel dient te worden nageleefd.

Doordat artikel 22 van de Grondwet aan de bevoegde wetgever de bevoegdheid voorbehoudt om vast te stellen in welke gevallen en onder welke voorwaarden afbreuk gedaan kan worden aan het recht op eerbiediging van het privéleven, waarborgt het aan elke burger dat geen enkele inmenging in 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 legaliteitsbeginsel 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.³¹

10.2. Bijgevolg moeten de essentiële elementen van de verwerking van persoonsgegevens in de wet zelf worden vastgelegd.³²

²⁹ Adv.RvS 63.192/2 van 19 april 2018 over een voorontwerp dat heeft geleid tot de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’, *Parl.St.* Kamer 2017-18, nr. 54-3126/001, 402-456, <http://www.raadvst-consetat.be/dbx/adviezen/63192.pdf>; adv.RvS 63.202/2 van 28 april 2018 over een voorontwerp dat heeft geleid tot 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’, *Parl.St.* Kamer 2017-18, nr. 54-3185/001, 120-145, <http://www.raadvst-consetat.be/dbx/adviezen/63202.pdf>.

³⁰ Artikel 8, § 2, van het EVRM.

³¹ Vaste rechtspraak van het Grondwettelijk Hof: zie inzonderheid GwH 18 maart 2010, nr. 29/2010, B.16.1; GwH 20 februari 2020, nr. 27/2020, B.17.

³² Zie inzonderheid adv.RvS 64.879/4 van 4 februari 2019 over een voorontwerp dat heeft geleid tot het decreet van het Waalse Gewest van 2 mei 2019 ‘tot wijziging van het Waalse Wetboek van Sociale Actie en Gezondheid wat betreft de preventie en de bevordering van de gezondheid’, *Parl.St.* W.Parl. 2018-19, nr. 1332/1, 25-35, <http://www.raadvst-consetat.be/dbx/adviezen/64879.pdf> en adv.RvS 66.443/1/V van 29 augustus 2019 over een ontwerp dat heeft geleid tot het koninklijk besluit van 9 februari 2020 ‘betreffende de registratie van wilsverklaringen over de wegneming van menselijk lichaamsmateriaal, met inbegrip van organen, na overlijden’, <http://www.raadvst-consetat.be/dbx/adviezen/66443.pdf>.

10.3. Het legaliteitsbeginsel inzake de verwerking van persoonsgegevens verzet zich tegen een al te vage omschrijving van de essentiële elementen van de regeling ter zake in het samenwerkingsakkoord.

Een aantal bepalingen van het samenwerkingsakkoord maken gewag van gegevens die “noodzakelijk” zijn om contact te leggen met de erin vermelde personen³³ of van gegevens of criteria die “relevant” zijn voor bepaalde situaties³⁴. Mede gelet op het belang van een snelle en adequate werking van de contactopsporing en de ermee gepaard gaande gegevensverwerking kan worden aanvaard dat de betrokken gegevens niet op uitputtende wijze in het samenwerkingsakkoord zelf worden opgesomd.

In artikel 9, § 1, 13°, van het samenwerkingsakkoord wordt gewag gemaakt van de “gegevens meegedeeld aan het contactcentrum, met inbegrip van symptomen, datum van de eerste symptomen, verplaatsingen, opvolging van isolatie- en hygiënemaatregelen”. Een dergelijke omschrijving van de te verwerken gegevens, die erop neerkomt dat alle gegevens die worden meegedeeld in aanmerking komen voor verwerking, is te ruim en moet uitdrukkelijk worden beperkt tot de gegevens die relevant zijn voor de contactopsporing. De omstandigheid dat die gegevens gepseudonimiseerd worden,³⁵ doet geen afbreuk aan die vaststelling.

10.4.1. Een aantal delegaties die in het samenwerkingsakkoord vervat zijn, hebben betrekking op essentiële elementen waarvan de regeling bij artikel 22 van de Grondwet aan de wetgever is voorbehouden.

Dat is meer bepaald het geval met:

– de machtiging vervat in artikel 11, § 4, van het samenwerkingsakkoord in zoverre daarbij de bevoegdheid wordt gedelegeerd om “de categorieën persoonsgegevens die in de gegevensbanken (...) worden verwerkt [te wijzigen of aan te vullen]”;

– de artikelen 11, § 3, en 12, § 1, van het samenwerkingsakkoord, waarbij de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité gemachtigd wordt om per verwerkingsdoeleinde de specifieke persoonsgegevens te definiëren en te preciseren die kunnen worden verwerkt en meegedeeld, evenals de nadere regels ter zake.³⁶

De afdeling Wetgeving heeft ter zake in advies 67.425/3-67.426/3-67.427/3 immers reeds het volgende opgemerkt:

“In zoverre de voorgestelde delegaties betrekking hebben op bijkomende categorieën van persoonsgegevens of op bijkomende doeleinden voor de verwerking van persoonsgegevens, moeten de beoogde categorieën en doeleinden in de tekst van het voorstel worden geregeld en kunnen ze niet worden gedelegeerd door de wetgever. Indien het daarentegen enkel gaat om de verdere concretisering van categorieën en doelstellingen

³³ Zie artikel 6, § 4, 12°, en § 5, 7°, artikel 7, § 2, 6°, en § 3, 7°, artikel 9, § 2, 8°, en artikel 14, § 4, tweede lid, van het samenwerkingsakkoord.

³⁴ Zie artikel 6, § 5, 9° en 10°, artikel 7, § 3, 9° en 10°, en artikel 9, § 2, 9°, van het samenwerkingsakkoord.

³⁵ Zie artikel 9, § 1, inleidende zin, van het samenwerkingsakkoord.

³⁶ Zie ook de bijzondere opmerking bij de artikelen 11 en 12.

die reeds in het voorstel worden bepaald, kan die concretisering worden gedelegeerd.³⁷”

Het samenwerkingsakkoord moet dienovereenkomstig worden herzien.

10.4.2. Bovendien hebben bepaalde aspecten van de delegatie die bij artikel 14, § 9, van het samenwerkingsakkoord wordt verleend aan een uitvoerend samenwerkingsakkoord wat betreft de nadere regels inzake de werking van de digitale contactopsporingsapplicatie, eveneens betrekking op essentiële elementen die krachtens artikel 22 van de Grondwet door de wetgever moeten worden geregeld.

Zo bijvoorbeeld zouden elementen als de beschrijving van de verwerkingen die voortvloeien uit het gebruik van de digitale contactopsporingsapplicatie (§ 9, 2°), de wijze waarop de gebruikers geïnformeerd worden (§ 9, 6°) en de controleprocedure (§ 9, 7°) beter moeten worden afgebakend in het voorliggende samenwerkingsakkoord.

Het samenwerkingsakkoord moet bijgevolg in dat opzicht worden aangepast en aangevuld.

2. Het beginsel van de minimale gegevensverwerking

11.1. Overeenkomstig artikel 5, lid 1, c), van de AVG moeten de persoonsgegevens die in aanmerking komen voor verwerking “toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt”. Dit beginsel van de minimale gegevensverwerking kwam volgens de Gegevensbeschermingsautoriteit in het gedrang door de “centralisatie van een grote hoeveelheid gezondheidsgegevens in één enkele gegevensbank die is opgezet, eigendom is van en wordt beheerd door een actor die slechts als tussenpersoon optreedt”.³⁸ De keuze voor de centralisatie van persoonsgegevens in de overkoepelende Gegevensbank I wordt door de gemachtigden als volgt verantwoord:

“De organisatie van de gegevensbanken is gebaseerd op principes van data protection by design, data protection by default en dataminimalisatie. Meervoudige opslag van dezelfde persoonsgegevens in gegevensbanken bij verschillende gefedereerde entiteiten is vermeden.

ICT-technisch heeft elke gegevensbank uiteraard een eigen onderliggend gegevensmodel. Verschillende gegevensmodellen geven aanleiding tot verschillende gegevensbanken. Zowel de GBA als de Raad van State hebben verzocht om het gegevensmodel van de onderscheiden gegevensbanken in detail te beschrijven, wat in het ontwerp van samenwerkingsakkoord is gebeurd.

Gegevensbank I is noodzakelijkerwijze een gemeenschappelijke gegevensbank over de gefedereerde entiteiten heen omdat het opvolgen van de contacten zich niet kan beperken tot de personen die ressorteren onder één deelstaat. Het organiseren van een gegevensbank per gefedereerde entiteit zou ertoe leiden dat elk gewest of een gemeenschap een eigen duplicaat van de gehele gegevensbank moet beheren, en er

³⁷ Voetnoot 15 van het geciteerde advies: Vgl. GwH 4 april 2019, nr. 49/2019, B.46.7 en B.47.2.

³⁸ Advies 42/2020 van de Gegevensbeschermingsautoriteit van 25 mei 2020, opmerking 3.

permanente synchronisatie zou moeten geschieden met het risico op datalekken. Dat is in strijd met principes van dataminimalisatie en informatieveiligheid voorzien in de AVG.

Daarenboven zou organiseren van een gegevensbank per gefedereerde entiteiten fundamentele, negatieve impact hebben op de omlooptijd binnen het gehele manuele contactonderzoek. Immers, de verschillende bewerkingen om de uitwisselingen van gegevens tussen de verschillende databanken van de deelstaten te organiseren, zou dermate veel tijd innemen dat dit het hele proces zou vertragen (van het opvolgen van personen die een test dienen te ondergaan tot het contacteren van de Personen Categorie II voor zover de test uitwees dat ze besmet zijn en Personen Categorie III).

De Gegevensbank III is een afzonderlijke gegevensbank die enkel de (bel)orders bevat voor de medewerkers van de contactcenters. Deze gegevensbank heeft een ander gegevensmodel dan Gegevensbank I en is dus een afzonderlijke gegevensbank. Overigens is een scheiding tussen Gegevensbank I en Gegevensbank III een maatregel van data protection by design om te vermijden dat de medewerkers van het contact center onnodige toegang zouden kunnen hebben tot de gezondheidsgegevens in Gegevensbank I. De Gegevensbank III is een gemeenschappelijke gegevensbank over de contact centers heen om dezelfde reden als gegevensbank I een gemeenschappelijke gegevensbank is over de gefedereerde entiteiten heen.

Gegevensbank IV is een afzonderlijke gegevensbank die informatie bevat over de contactpersonen van te contacteren collectiviteiten. Deze Gegevensbank heeft een ander gegevensmodel dan Gegevensbank I en Gegevensbank III en is dus een afzonderlijke gegevensbank.”

Het verdient aanbeveling om deze verantwoording mee op te nemen in de algemene toelichting bij het voorontwerp van instemmingstekst.

11.2. In vergelijking met de koninklijke besluiten en het wetsvoorstel vermeld in opmerking 3, worden meer te verwerken persoonsgegevens opgesomd in het samenwerkingsakkoord. De gemachtigden gaven hiervoor de volgende verantwoording:

“Men heeft hier willen voldoen aan een opmerking van de GBA. De GBA was bezorgd omdat het niet duidelijk was welke concrete persoonsgegevens werden gevraagd. Omwille van deze reden, werd naast het oplijsten van de categorieën van persoonsgegevens (hetgeen onder de AVG zou moeten volstaan) ook reeds voorzien in een oplijsting van de persoonsgegevens die onder een bepaalde categorie vallen. Het samenwerkingsakkoord gaat in de praktijk aldus niet verder dan initieel voorzien in het KB nr. 18. Er is wel sprake van een meer gedetailleerde beschrijving van de werkelijke gang van zaken. Dit teneinde tegemoet te komen aan de transparantievereiste van de AVG.”

Op het eerste gezicht kan worden aangenomen dat ook de toegevoegde persoonsgegevens voldoen aan het beginsel van de minimale gegevensverwerking.

11.3. Zoals blijkt uit de algemene toelichting en uit het dispositief van het samenwerkingsakkoord, is het niet de bedoeling dat de digitale contactopsporing het manuele contactonderzoek vervangt, maar wel dat het dat manuele contactonderzoek aanvult. Gelet op de grootschalige verwerking van gegevens die gepaard gaat met het gebruik van de digitale contactopsporingsapplicatie, moet bijgevolg kunnen worden aangetoond dat dat gebeurt in overeenstemming met het beginsel van de minimale gegevensverwerking.

In advies 67.424/3 heeft de Raad van State reeds opgemerkt dat, gelet op het vrijwillige karakter van de digitale contactopsporingsapplicaties, de werkzaamheid ervan staat of valt met een voldoende hoge dekkingsgraad, met andere woorden met het aantal burgers dat de applicatie in gebruik neemt.³⁹ Die dekkingsgraad zal bepalend zijn voor de mate waarin de applicaties daadwerkelijk een complementaire rol kunnen spelen naast de manuele contactopsporing die door de bevoegde overheden wordt geïmplementeerd. Daarbij moet ook rekening worden gehouden met de grootschalige verwerking van persoonsgegevens die gepaard gaat met het gebruik van die applicaties. Die verwerking moet immers, overeenkomstig het zo-even aangehaalde beginsel van de minimale gegevensverwerking, beperkt zijn tot wat noodzakelijk is voor de beoogde doeleinden. Het komt er dus op aan dat noodzakelijkheidsbeginsel te verzoenen met een voldoende hoge dekkingsgraad.

In dat verband moet ook worden gewezen op de gegevensbeschermingseffectbeoordeling die de verwerkingsverantwoordelijke moet uitvoeren voor het begin van de verwerkingsactiviteiten, overeenkomstig artikel 35 van de AVG, “[w]anneer 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”. Dat is hier ook het geval,⁴⁰ zoals trouwens wordt bevestigd in artikel 14, § 8, van het samenwerkingsakkoord, zodat die effectbeoordeling hoe dan ook zal moeten worden uitgevoerd, bij voorkeur vooraleer de parlementaire instemming wordt verleend.

In tegenstelling tot het in opmerking 4 aangehaalde wetsvoorstel wordt in het samenwerkingsakkoord niet voorzien in een evaluatie van de regeling in het samenwerkingsakkoord zelf. In advies 67.424/3 werd het belang van zo’n evaluatie benadrukt, “[a]angezien het hier gaat om een nieuwe technologie en gelet op het belang van een nauwgezette opvolging van de zo-even geschetste afweging tussen een voldoende hoge dekkingsgraad en het noodzakelijkheidsbeginsel van de met de applicaties gepaard gaande verwerking van persoonsgegevens”. Het ontbreken van een dergelijke evaluatieverplichting in het samenwerkingsakkoord werd door de gemachtigden als volgt verantwoord:

“Aangezien het samenwerkingsakkoord slechts een algemeen kader voorziet voor de contactopsporingsapplicatie, dat dan verder door de deelstaten moet ingevuld worden, is een vorm van evaluatie niet aan de orde. De evaluatie zal immers moeten plaatsvinden op het niveau van de deelstaten. Gelieve te willen noteren dat na deze crisis een evaluatie van de gehele aanpak van deze crisis zal gebeuren, derhalve ook van het proces van het manuele contactonderzoek tot het inzetten van een digitale contactopsporingsapplicatie.”

11.4. In het licht van de inachtneming van het beginsel van de minimale gegevensverwerking rijst bovendien de vraag hoe ervoor kan worden gezorgd dat de regelgeving inzake digitale contactopsporing wordt nageleefd. Het voorliggende samenwerkingsakkoord bepaalt zich ertoe het aan een uitvoerend samenwerkingsakkoord over te laten om te voorzien in “de procedure voor de controle op de goede werking van de contactopsporingsapplicatie”.⁴¹ In

³⁹ Zie <https://ukhumanrightsblog.com/2020/05/01/what-are-the-data-privacy-considerations-of-contact-tracing-apps/>.

⁴⁰ In die zin ook advies nr. 34/2020 van 28 april 2020 van de Gegevensbeschermingsautoriteit, opmerkingen 23 en 48.

⁴¹ Artikel 14, § 9, 7°, van het voorliggende samenwerkingsakkoord.

dat verband heeft de afdeling Wetgeving reeds het volgende opgemerkt: “Er kan wellicht beter worden voorzien in administratieve sancties of strafsancties voor het aanbieden van niet-conforme applicaties.”⁴²

11.5. In het licht van de inachtneming van het beginsel van de minimale gegevensverwerking rijst ook de vraag wanneer er een einde komt aan de digitale contactopsporing.

In dat verband staat in artikel 14, § 3, 10°, van het samenwerkingsakkoord het volgende:

“De centrale loglijst in Gegevensbank V wordt in elk geval gedeactiveerd zodra door een uitvoerend samenwerkingsakkoord als bedoeld bij artikel 92bis, § 1, derde lid, van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen, is vastgesteld dat deze niet meer nodig zijn voor het beheer van de beëindiging van de exitstrategie; de centrale loglijst wordt ten laatste automatisch gedeactiveerd na 1 jaar, tenzij door een uitvoerend samenwerkingsakkoord wordt beslist dat een verlenging van deze periode noodzakelijk is.”

De stellers van het samenwerkingsakkoord moeten kunnen uitleggen waarom de voorziene deactivering enkel betrekking heeft op de centrale loglijst en niet op de digitale contactopsporingsapplicatie in haar geheel.

Teneinde aan het vereiste van evenredigheid te voldoen, dient meer in het algemeen voor alle maatregelen waarin het samenwerkingsakkoord voorziet exact te worden bepaald tot wanneer ze geldig zijn.⁴³

3. Het beginsel van integriteit en van vertrouwelijkheid

12. De inachtneming van het beginsel van integriteit en van vertrouwelijkheid (artikel 5, lid 1, f), van de AVG) vereist ten slotte dat voldoende garanties geboden worden ter voorkoming van elk misbruik van die inmenging in het privéleven.

Het samenwerkingsakkoord bevat verscheidene garanties ter voorkoming van elk misbruik, zoals het feit dat de “broncode” openbaar gemaakt wordt, dat het gebruik van de digitale applicatie op vrijwillige basis gebeurt, dat het niet-gebruiken van de applicatie geen aanleiding geeft tot enig nadeel en dat de gebruikers van de applicatie niet worden geïdentificeerd.

De vraag rijst evenwel of die verschillende garanties volstaan om elk misbruik te voorkomen en om de inmenging zoveel mogelijk te beperken.

Het samenwerkingsakkoord verplicht het gebruik van het “DP3T”-protocol. In de algemene toelichting staat dat dat systeem ervoor zou moeten zorgen “dat de inmenging op het

⁴² Adv.RvS 67.424/3, opmerking 15.2.

⁴³ Zie de bijzondere opmerking bij artikel 19.

vlak van het privéleven wordt geminimaliseerd”. Zoals de Gegevensbeschermingsautoriteit opmerkt zou die toelichting evenwel moeten worden aangevuld met uitleg “over de essentiële onderdelen van het DP3T-protocol, de garanties die het biedt, de restrisico’s en de redenen waarom geconcludeerd moet worden dat de gegevensverwerkingen die zouden worden uitgevoerd toch proportioneel zijn”.⁴⁴

De afdeling Wetgeving stelt niet alleen vast dat de werkwijze moeilijkheden doet rijzen in het licht van het legaliteitsbeginsel,⁴⁵ maar ook dat het samenwerkingsakkoord het aan een toekomstig uitvoerend samenwerkingsakkoord overlaat om verschillende garanties te definiëren: de beschrijving van het opsporingssysteem, de definities van belangrijke begrippen zoals het risicocontact, de autorisatiecode, de beveiligde sleutel en het niet-gepersonaliseerd tijdelijk serienummer,⁴⁶ de specifieke garanties om het risico van heridentificatie te beperken en de wijze waarop de betrokkenen geïnformeerd zullen worden over de werking van de digitale toepassing en de procedure voor de controle op de goede werking ervan (artikel 14, § 9, van het voorliggende samenwerkingsakkoord).

Daaruit volgt dat de afdeling Wetgeving niet in staat is in dit stadium te beoordelen of voldoende garanties geboden zullen worden om elk misbruik te voorkomen bij het gebruik van de digitale contactopsporingapplicaties.

C. Overeenstemming van de Franse en de Nederlandse tekst van het samenwerkingsakkoord

13. De tekst van het samenwerkingsakkoord bevat heel wat taalkundige slordigheden. Het samenwerkingsakkoord dient dan ook nog aan een grondig redactioneel en taalkundig nazicht te worden onderworpen, in het bijzonder met betrekking tot de overeenstemming tussen de Nederlandse en Franse tekst.

Bij wijze van voorbeeld kan op het volgende worden gewezen:

– in de Franse tekst van artikel 2, § 5, van het samenwerkingsakkoord moet de vermelding “41ompétente sou” telkens worden vervangen door “compétentes ou”;

– in de Nederlandse tekst van artikel 3, § 1, 3°, *in fine*, van het samenwerkingsakkoord moet worden verwezen naar artikel 10, § 2, in plaats van naar artikel 11, § 2;

⁴⁴ Advies 43/2020, 16.

⁴⁵ Zie hiervoor de opmerking over de inachtneming van het legaliteitsbeginsel.

⁴⁶ In dat verband heeft de Gegevensbeschermingsautoriteit ook het volgende opgemerkt: “Bovendien houdt het minimaliseringsbeginsel van de AVG in dat alleen gegevens mogen worden verwerkt die strikt noodzakelijk en relevant zijn voor het nagestreefde doel. Gelet op de definitie van risicocontacten die door de FOD Volksgezondheid en het Crisiscentrum is vastgesteld (contact van minder dan 1,5 meter met een besmette persoon gedurende meer dan 15 minuten), is de Autoriteit dan ook van oordeel dat alleen dergelijke contacten (in voorkomend geval met een aanvaardbare foutmarge van het type ‘contact van minder dan 4 meter afstand voor meer dan 10 minuten’) moeten worden opgevangen (vooral omdat de Bluetooth-technologie het mogelijk maakt contacten tot 100 meter afstand op te vangen, wat duidelijk disproportioneel is voor het nagestreefde doel). De formulering van het doeleinde zal op deze basis moeten worden herzien en met het oog op de rechtszekerheid moet een definitie van het begrip ‘risicocontact’ overeenkomstig de officiële aanbevelingen in artikel 3 van het wetsontwerp worden” opgenomen (advies 43/2020, punt 27).

– in de Nederlandse tekst van artikel 10, § 3, van het samenwerkingsakkoord moet “Gegevensbank I” geschreven worden in plaats van “Gegevensbank”.

BIJZONDERE OPMERKINGEN

AANHEF

14. Aangezien het derde lid geen rechtsgrond biedt voor het samenwerkingsakkoord, moet het worden weggelaten of in de vorm van een overweging worden opgenomen.

15. Het tiende lid is een nodeloze herhaling van het vierde lid en moet bijgevolg worden weggelaten.

16. Het vijftiende lid moet worden weggelaten aangezien koninklijk besluit nr. 18 van 4 mei 2020 ‘tot oprichting van een databank bij Sciensano in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19’ op 30 juni 2020 buiten werking is getreden.

DISPOSITIEF

Artikel 1

17.1. In de definitie van “clusters” in artikel 1, § 1, 2°, van het samenwerkingsakkoord moeten de woorden “collectiviteiten of gemeenschappen” worden vervangen door het woord “collectiviteiten”, aangezien de term “gemeenschap” al voorkomt in de definitie van “collectiviteit” in artikel 1, § 1, 3°.

17.2. In artikel 1, § 1, 6°, van het samenwerkingsakkoord wordt gewag gemaakt van een samenwerkingsovereenkomst gesloten tussen het RIZIV en Sciensano. De gemachtigden verklaarden dat daarmee wordt verwezen naar de gegevensbank bij Sciensano die is opgericht ter uitvoering van een samenwerkingsovereenkomst met het RIZIV, bedoeld in artikel 22, 20°, van de wet ‘betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen’, gecoördineerd op 14 juli 1994.⁴⁷ De verwijzing naar die wetsbepaling kan duidelijkheidshalve beter worden opgenomen.

Die opmerking geldt ook voor artikel 3, § 1, 4°, en artikel 15, § 2, van het samenwerkingsakkoord.

18. Overeenkomstig artikel 1, § 6, tweede lid, van het samenwerkingsakkoord zijn “in afwijking van artikel 458 van het Strafwetboek (...) de gecontacteerde personen ontheven van hun geheimhoudingsplicht uit hoofde van dit samenwerkingsakkoord”. Er zou, in het licht van het strafrechtelijk legaliteitsbeginsel, meer precies moeten worden geformuleerd om welke personen het gaat. De gemachtigden lieten alvast weten dat het gaat om de personen die door de

⁴⁷ Toegevoegd bij de wet van 10 april 2014 ‘houdende diverse bepalingen inzake gezondheid’.

contactcentra worden gecontacteerd, namelijk de Personen Categorie II voor zover de COVID-19-test uitwees dat ze besmet zijn, alsook de Personen Categorie III.

Artikel 3

19. In artikel 3, § 2, 2°, B, van het samenwerkingsakkoord wordt melding gemaakt van de Personen Categorie V en VI, terwijl in artikel 7, § 4, van het samenwerkingsakkoord, waarnaar wordt verwezen, enkel melding wordt gemaakt van de Personen Categorie VI. De gemachtigden erkennen dat het om een materiële vergissing gaat, die moet worden rechtgezet.

20. Door zijn formulering wekt artikel 3, § 3, van het samenwerkingsakkoord de indruk dat de bevoegde mobiele teams en gezondheidsinspectiediensten geen persoonsgegevens van de Personen Categorie IV mogen verwerken. De stellers van het samenwerkingsakkoord moeten nagaan of dit de bedoeling is en in voorkomend geval de betrokken bepaling aanpassen.

Artikel 6

21. In artikel 6, §§ 2 en 4, van het samenwerkingsakkoord wordt verwezen naar het INSZ-nummer en naar het identificatienummer van het Rijksregister. De keuze voor het gebruik van die identificatienummers⁴⁸ wordt als volgt gerechtvaardigd in de algemene toelichting bij het samenwerkingsakkoord:

“Met het oog op de eenduidige identificatie van de betrokken personen (zijnde gehospitaliseerde patiënten, besmette personen of personen van wie een ernstig vermoeden bestaat dat zij besmet zijn) en het onderling linken van de verzamelde gegevens, is het absoluut noodzakelijk om ook het identificatienummer van de sociale zekerheid van de betrokken personen wiens gegevens in de Gegevensbank I worden verwerkt op te slaan en te voorzien in een algemene toegang tot het Rijksregister. Tevens ontlast dit de artsen, ziekenhuizen en laboratoria die de informatie ter beschikking stellen (d.i. de informanten), aangezien zij enkel de gegevens dienen aan te leveren die niet kunnen worden teruggevonden in het Rijksregister. Gelet op het feit dat het hele gezondheidszorgsysteem in België gebaseerd is op het gebruik van het rijksregisternummer om een patiënt daadwerkelijk te kunnen identificeren, is ook dit nummer van noodzakelijk belang om te verwerken binnen het manuele contactonderzoek, met het oog op het juist identificeren van de indexpersoon alsook van de personen met wie de indexpersoon in contact is geweest.”

De gemachtigden verstrekten nog de volgende bijkomende toelichting:

“Het verplicht gebruik van het identificatienummer van de sociale zekerheid als uniek identificatienummer in de gezondheidssector is overigens geregeld door artikel 8 van de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealthplatform. Het Grondwettelijk Hof heeft in zijn arrest 29/2010 van 18 maart 2010 geoordeeld dat ‘rekening houdend met de waarborgen waarin de wet van 21 augustus 2008 voorziet met betrekking tot de vertrouwelijkheid van de persoonlijke gezondheidsgegevens gedurende de verwerking ervan door het eHealth-platform, is de

⁴⁸ Zie ook de kritiek in advies 42/2020 van de Gegevensbeschermingsautoriteit van 25 mei 2020, opmerking 19.

keuze om gebruik te maken van het rijksregisternummer, als identificatiesleutel, in redelijkheid verantwoord'."

Zoals de gemachtigden ook zelf suggereerden, kan die bijkomende toelichting beter worden opgenomen in de voormelde algemene toelichting.

22. In artikel 6, § 4, van het samenwerkingsakkoord schrijve men allicht "Gegevensbank III" in plaats van "Gegevensbank I".

23. Artikel 6, § 5, 7°, van het samenwerkingsakkoord vermeldt als een van de categorieën van de in Gegevensbank I te verwerken persoonsgegevens "de gegevens noodzakelijk voor het contactcentrum om verder nuttig contact te leggen met de persoon bedoeld in deze paragraaf en de lijst met personen waarmee de persoon bedoeld in deze paragraaf recent contact heeft gehad, met inbegrip van postcode en taal en het ingeschatte besmettingsrisico van de persoon bedoeld in deze paragraaf".

Het is evenwel niet duidelijk wat het verband is tussen de contactgegevens van de betrokken personen en het ingeschatte besmettingsrisico. Bovendien lijkt dat laatste gegeven te overlappen met hetgeen wordt vermeld in artikel 6, § 5, 9°, van het samenwerkingsakkoord.

Die opmerking geldt *mutatis mutandis* ook voor artikel 7, § 3, 7° en 9°, van het samenwerkingsakkoord.

Artikel 8

24. In artikel 8, 1°, van het samenwerkingsakkoord wordt gewag gemaakt van het "identificatienummer uit authentieke bron". De gemachtigden verklaarden dat daarmee het Rijksregister en de Kruispuntbank van de sociale zekerheid worden bedoeld. Dit kan beter worden verduidelijkt.

Artikel 10

25. De gemachtigden bevestigden dat in artikel 10, § 1, van het samenwerkingsakkoord verkeerdelijk wordt gerefereerd aan de Personen Categorie V. De vermelding van die categorie moet dan ook worden weggelaten.

26. De gemachtigden bevestigden eveneens dat de algemene vermelding van "infectieziekten" in artikel 10, § 2, van het samenwerkingsakkoord verkeerd is en dat specifiek melding moet worden gemaakt van COVID-19.

Artikelen 11 en 12

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,⁴⁹ 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-beleidsmatige 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.⁵⁰

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.

28. Benevens de voorgaande opmerkingen zou de strekking van artikel 11 van het samenwerkingsakkoord moeten worden verduidelijkt.

⁴⁹ Zie in dat verband trouwens ook de kritiek die de Raad van State ter zake reeds had geformuleerd in adv.RvS 63.202/2 van 26 april 2018 over een voorontwerp dat heeft geleid tot 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', *Parl.St.* Kamer 2017-18, nr. 54-3185/001, 140-142.

⁵⁰ Vergelijk met de toetsingscriteria die het Grondwettelijk Hof gebruikt om delegaties van verordenende bevoegdheid door de wetgever aan een autonome administratieve overheid of een gedecentraliseerde openbare instelling te beoordelen; zie GwH 11 juni 2015, nr. 86/2015, B.22.4 en GwH 9 juni 2016, nr. 89/2016, B.9.6.4: "De artikelen 33, 105 en 108 van de Grondwet verzetten zich niet er tegen dat, in een bepaalde technische materie, de wetgever specifieke uitvoerende bevoegdheden toevertrouwt aan een autonome administratieve overheid die zowel aan de jurisdictionele controle als aan de parlementaire controle is onderworpen, en verbieden de wetgever niet om delegaties te verlenen aan een uitvoerend orgaan, op voorwaarde dat die betrekking hebben op de uitvoering van maatregelen waarvan het doel door de bevoegde wetgever is bepaald, in het bijzonder in technische en ingewikkelde materies."; zie GwH 19 november 2015, nr. 162/2015, B.8.4: "Artikel 33 van de Grondwet en artikel 20 van de bijzondere wet van 8 augustus 1980 [tot hervorming der instellingen] staan niet eraan in de weg dat de wetgever specifieke uitvoerende bevoegdheden toevertrouwt aan een gedecentraliseerde openbare instelling die aan een bestuurlijk toezicht en aan een rechterlijke toetsing is onderworpen."

Zowel de afdeling Wetgeving als de Gegevensbeschermingsautoriteit vragen zich immers af wat moet worden verstaan onder:

“Voor zover niet opgenomen in dit samenwerkingsakkoord, gebeurt zowel de mededeling van persoonsgegevens aan Sciensano voor verwerking in de Gegevensbank I, als de verdere mededeling van die persoonsgegevens door Sciensano aan derden, steeds na beraadslaging door de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité (...).”

De Gegevensbeschermingsautoriteit maakte de volgende opmerking:

“Moet elke zorgverlener (dus ook elke arts) of gezondheids- of zorgorganisatie elk van zijn mededelingen systematisch onderwerpen aan een beraadslaging van het informatieveiligheidscomité? Deze aanpak lijkt administratief erg omslachtig. Of is het een beraadslaging per broncategorie en wat zijn dan de verschillende categorieën?”⁵¹

Ter wille van de rechtszekerheid moet de formulering van artikel 11 worden herzien.

29. Artikel 12, § 3, van het samenwerkingsakkoord vereist een beraadslaging van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité “voor zover de mededeling van deze bijkomende persoonsgegevens nodig is voor de verwerkingsdoeleinden bepaald in artikel 3”.

Die bepaling is te vaag geformuleerd.

Indien de bepaling behouden blijft, moet ze worden herzien teneinde erin te vermelden dat de toestemming alleen kan worden verleend op voorwaarde dat de mededeling van de bijkomende persoonsgegevens noodzakelijk is voor de in artikel 3 gedefinieerde verwerkingsdoeleinden.

Artikel 14

30. Ter wille van de rechtszekerheid moet de terminologie die in artikel 14 van het samenwerkingsakkoord wordt gebruikt om te verwijzen naar “de digitale contactopsporingsapplicatie”, worden geüniformiseerd.

Aangezien “Gegevensbank V” in artikel 1, punt 9°, wordt gedefinieerd als “de centrale loglijst (...)”, is het voorts niet nodig om in artikel 14 te verwijzen naar de “centrale loglijst in Gegevensbank V”.⁵² Het volstaat te verwijzen naar de Gegevensbank V.

31. In artikel 14 wordt niet gespecificeerd wie toegang zal hebben tot de Gegevensbank V. Als dit alleen de verwerkingsverantwoordelijke is, namelijk Sciensano, dient dat uitdrukkelijk te worden vermeld.

⁵¹ Advies 36/2020, punt 36.

⁵² Zie met name artikel 14, § 3, 3°, 9° en 10°.

Zoals de Gegevensbeschermingsautoriteit voorts opmerkt “moet ook duidelijk worden gespecificeerd welke gegevensverwerking door Sciensano wordt uitgevoerd om de werking van het opsporingssysteem te garanderen”.⁵³

32. Artikel 14, § 2, 2°, voorziet in de door een gebruiker “op een geanonimiseerde, minstens gepseudonimiseerde, wijze” gemelde COVID-19-besmetting.

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

Op de vraag of een pseudonisering noodzakelijk is, hebben de gemachtigden het volgende geantwoord:

“Technisch gezien zou men kunnen stellen dat de beveiligde sleutels die gebruikt worden op het toestel van de gebruiker en eigen zijn aan een gebruiker, alsnog (en enkel door gebruik te maken van hacking-technieken) zouden kunnen toelaten om de gedeelde serienummers van diezelfde gebruiker te ontsleutelen en terug te koppelen aan die gebruiker. Dus hoewel eerder theoretisch van aard, bestaat er dus nog een sleutel, vandaar dat de gegevens eerder als gepseudonimiseerd moeten beschouwd worden, dan geanonimiseerd. De toegang tot deze beveiligde sleutels is afgeschermd, ook voor de gebruiker. Enkel met toegang tot het toestel en de nodige hackingtechnieken zou men eventueel in staat kunnen zijn om de sleutel te achterhalen. Het enige wat daar dan nog uit zou kunnen geleerd worden, is of de gebruiker zich gemeld heeft als besmette gebruiker of niet. Centraal kan er echter niets ontsleuteld worden. Ook andere gebruikers kunnen op geen enkele manier de gedeelde serienummers terugkoppelen aan een individu.”

In het licht van dat antwoord lijkt de voorliggende bepaling aanvaardbaar.

33. In artikel 14, § 3, 2°, zou moeten worden gepreciseerd wat wordt verstaan onder een mobiele applicatie die “lokaal” wordt geïnstalleerd.

In punt 14° van dezelfde paragraaf zou, ter wille van de rechtszekerheid, minstens in de algemene toelichting moeten worden gespecificeerd wat wordt verstaan onder de “volledige broncode” en de “toepassingslaag”. De formulering van die bepaling moet bovendien worden herzien.

34. Artikel 14, § 5, eerste lid, bepaalt dat het installeren, het gebruiken en het de-installeren van de digitale contactopsporingsapplicatie door een gebruiker uitsluitend op vrijwillige basis gebeuren.

⁵³ Advies 43/2020, punt 25.

In dat verband heeft de afdeling Wetgeving eerder al het volgende opgemerkt:

“De vraag rijst evenwel of die bepaling in haar algemene formulering voldoende rekening houdt met artikel 8 van de AVG, dat voorwaarden bepaalt voor de toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij en dat voorschrijft dat voor kinderen jonger dan 16 jaar (of eventueel tot jonger dan 13 jaar)⁵⁴ de toestemming of machtiging tot toestemming is vereist van de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt. De verwerkingsverantwoordelijke moet, met inachtneming van de beschikbare technologie, redelijke inspanningen doen om te controleren of die vereiste (machtiging tot) toestemming is gegeven. Ook al is de voormelde verordeningsbepaling rechtstreeks toepasselijk en is ze dus bindend voor de verwerkingsverantwoordelijke, toch kan worden overwogen om het wetsvoorstel aan te vullen met bepalingen die die eis concretiseren voor de betrokken applicatie.”⁵⁵

Een dergelijke opmerking kan ook hier worden gemaakt.

35. Artikel 14, § 5, tweede lid, bepaalt dat “[het] al dan niet installeren, het al dan niet gebruiken en het al dan niet de-installeren van de mobiele applicatie van de digitale contactopsporingsapplicatie geen aanleiding kan geven (...) tot enig voordeel of nadeel”.

In dat verband heeft de afdeling Wetgeving eerder al het volgende opgemerkt:

“Het op sluitende wijze omschrijven van de term ‘enig voordeel of nadeel’ in de tekst van het voorstel zelf is allicht onmogelijk, maar dat neemt niet weg dat het op basis van de huidige tekst en de toelichting erbij niet duidelijk is of de applicatie bijvoorbeeld gebundeld kan worden met andere, voor de gebruiker interessante toepassingen, of dat aan het gebruik van de applicatie bepaalde kortingen kunnen worden verbonden, enzovoort. Het is dan ook raadzaam om de casuïstiek toch enigszins te schetsen naar aanleiding van de parlementaire bespreking.”⁵⁶

Daarover om uitleg gevraagd, hebben de gemachtigden de volgende verduidelijkingen gegeven:

“Een werkgever mag bijvoorbeeld zijn werknemers niet verplichten om de contactopsporingsapplicatie te installeren. Dit mag op geen enkele wijze geschieden, en aldus ook niet door daar bepaalde voor- of nadelen te koppelen aan het al dan niet installeren van de contactopsporingsapplicatie. Zo zal het bijvoorbeeld niet toegelaten zijn om een werknemer een bonus te geven voor het installeren van de contactopsporingsapplicatie(...), of een deel van het loon in te houden ten gevolge van het niet installeren van de app, of werknemers de toegang tot de gebouwen te ontfemen bij niet gebruik van de contactopsporingsapplicatie. Leveranciers van goederen en diensten mogen het gebruik of niet gebruik van de contactopsporingsapplicatie niet linken aan hun goederen of diensten of een voorwaarde maken voor het verkrijgen van hun goederen en diensten. Bijvoorbeeld kortingen aanbieden bij gebruik van de app, toegang weigeren bij niet gebruik van de app (bioscoop, luchthaven, winkel, openbaar vervoer, taxi, vliegtuig, horeca, enz.).

⁵⁴ Voetnoot 29 van het geciteerde advies: Indien ervoor wordt gekozen om een lagere leeftijd dan 16 jaar te hanteren overeenkomstig artikel 8, lid 1, tweede alinea, van de AVG.

⁵⁵ Adv.RvS 67.424/3.

⁵⁶ Ibidem.

Indien gewenst kan dit verder worden toegelicht in de algemene toelichting van het samenwerkingsakkoord.”

Met dergelijke verduidelijkingen is het inderdaad mogelijk de draagwijdte van de uitdrukking “enig voordeel of nadeel” beter in te schatten. Die verduidelijkingen moeten opgenomen worden in de algemene toelichting.

36. Er wordt verwezen naar de bijzondere opmerking betreffende artikel 15, wat de motivering betreft van de keuze voor een termijn van drie weken.

37. Onder de doelstellingen die met de verwerking van de persoonsgegevens nagestreefd worden, wordt in artikel 14, § 2, niet uitdrukkelijk melding gemaakt van de aanvullende verwerking van persoonsgegevens met het oog op wetenschappelijk en epidemiologisch onderzoek. Met de digitale contactopsporingsapplicatie wordt dus blijkbaar geen enkele doelstelling inzake epidemiologisch onderzoek nagestreefd.⁵⁷

Artikel 14, § 7, tweede lid, voorziet evenwel in de mogelijkheid de verzamelde informatie

“overeenkomstig de voorwaarden bepaald in Titel 4 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens [te verwerken] met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden bedoeld in artikel 89, §§ 2 en 3 van de [AVG]”.

Op een vraag in dat verband hebben de gemachtigden het volgende antwoord gegeven:

“Enkel het loutere antwoord op de vraag of men al dan niet gebruik maakt van een applicatie zal worden meegenomen in de gegevensuitwisseling naar Gegevensbank II. Het bewaren van bijkomende gegevens, louter met het oog op wetenschappelijk onderzoek en ingeval van een opt-in door de gebruiker, werd bij de uitwerking van dit akkoord niet langer opportuun geacht, onder meer omwille van de bezorgdheid om een duidelijke communicatie ten aanzien van de burger te kunnen voeren met betrekking tot de doelstellingen van de applicatie.”

Als dat de bedoeling is, moet artikel 14, § 7, tweede lid, worden weggelaten.

38. Artikel 14 dient aldus te worden aangevuld dat daarin wordt bepaald wie belast wordt met het nemen van de beslissing welke applicatie(s) ter beschikking van het publiek zal/zullen worden gesteld na controle van hun overeenstemming met de regels bepaald in dit samenwerkingsakkoord⁵⁸ en wie naderhand belast zal worden met het uitschakelen van die applicaties zodra de termijn verstreken is waarbinnen daarvan op geldige wijze gebruikgemaakt kon worden.⁵⁹

⁵⁷ Zoals de Gegevensbeschermingsautoriteit had aangeraden (zie advies 43/2020, punt 30).

⁵⁸ Zie in dezelfde zin advies 43/2020 van de Gegevensbeschermingsautoriteit, punt 21.

⁵⁹ *Ibidem*, punt 35.

Artikel 15

39.1. Naar het voorbeeld van wat in de algemene toelichting bij het samenwerkingsakkoord vermeld staat met betrekking tot de bewaringstermijn van zestig dagen waarvoor gekozen is voor de gegevens in de Centrale Gegevensbank, zou de keuze moeten worden verantwoord van de bewaringstermijnen die voor de persoonsgegevens uit de overige Gegevensbanken is gemaakt.

In het bijzonder wordt in artikel 15, § 1, eerste lid, van het samenwerkingsakkoord bepaald dat de persoonsgegevens uit de Gegevensbank IV ofwel om de tien jaar geüpdatet ofwel gewist worden. Op een vraag in dat verband hebben de gemachtigden het volgende geantwoord:

“Na een termijn van 10 jaar worden de gegevens ofwel gewist, ofwel nagekeken op hun accuraatheid en indien nodig geüpdatet. Indien in geval van niet-accurate gegevens updaten onmogelijk is of niet opportuun, zullen de gegevens gewist worden. Zolang ze niet gewist zijn, zijn ze accuraat en zijn dit de gegevens van de contactpersonen van de collectiviteiten. In geval van uitbraken van andere infectieziekten, zal dit immers zeer nuttig zijn.”

Dat aldus voor die persoonsgegevens niet wordt voorzien in een maximale bewaringstermijn, is evenwel niet conform artikel 5, lid 1, e), van de AVG, naar luid waarvan

“persoonsgegevens (...) bewaard [moeten worden] in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan [noodzakelijk is] voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.”⁶⁰

39.2. Op de vraag wat de redenen zijn voor de uitzondering die volgens paragraaf 1, tweede lid, gemaakt wordt, wat de Gegevensbanken IV en V betreft, hebben de gemachtigden het volgende geantwoord:

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

Het dispositief moet aldus worden herzien dat het beantwoordt aan het beginsel dat het aan de wetgever staat om de bewaringstermijnen voor de persoonsgegevens vast te stellen.

39.3. De gemachtigden hebben geen enkele verantwoording gegeven voor de uitzondering die voor de Gegevensbank V wordt gemaakt. Bij gebrek aan verantwoording dient bijgevolg een soortgelijke bepaling als paragraaf 1, tweede lid, te worden opgenomen voor het wissen van de persoonsgegevens uit de Gegevensbank V.

⁶⁰ Zie ook de adv.RvS 37.748/AV en 37.749/AV van 23 november 2004 over een voorontwerp dat heeft geleid tot de wet van 3 mei 2005 ‘houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen’ (37.748/AV) en over een voorontwerp dat heeft geleid tot de wet van 3 mei 2005 ‘houdende wijziging van de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen’ (37.749/AV), *Parl.St.* Kamer 2004-05, nrs. 51-1598/001 en 51-1599/001, 45-77, <http://www.raadvst-consetat.be/dbx/adviezen/37748.pdf>.

40. In paragraaf 2 dient te worden vermeld naar welke bepalingen van de wet van 10 april 2014 ‘houdende diverse bepalingen inzake gezondheid’ daarin wordt verwezen.

Op een vraag in dat verband hebben de gemachtigden het volgende geantwoord:

“Hiermee wordt naar artikel 16 van de wet van 10 april 2014 verwezen.”

Paragraaf 2 moet bijgevolg in die zin worden aangevuld.

Artikel 16

41. Op een vraag betreffende de draagwijdte van artikel 16, § 4, van het samenwerkingsakkoord hebben de gemachtigden het volgende geantwoord:

“Hier wordt een overeenkomst bedoeld die enerzijds elementen heeft van de overeenkomst die normaal wordt afgesloten tussen de verwerkingsverantwoordelijke en de verwerker, en anderzijds een overeenkomst die normaal wordt afgesloten tussen verschillende verwerkingsverantwoordelijken voor de overdracht van persoonsgegevens.

Het uitgangspunt van een dergelijke overeenkomst tussen Sciensano en de deelstaten is dat er een gemeenschappelijk beleid is inzake het tegemoetkomen aan de rechten van de betrokkenen. Immers, onder de AVG heeft elke verwerkingsverantwoordelijke de plicht om te reageren op verzoeken van de betrokkene omtrent zijn of haar rechten. Hierbij kan gedacht worden aan bijvoorbeeld het recht op inzage. Echter, omwille van het feit dat het voor de betrokkene weinig opportuun is om zijn of haar verzoek te richten aan elke verwerkingsverantwoordelijke afzonderlijk, moeten hiervoor afspraken worden gemaakt tussen de verwerkingsverantwoordelijken onderling. In de overeenkomst kan bijvoorbeeld worden bepaald dat één partij optreedt als een single point of contact die alle verzoeken van de betrokkenen behandelt.”

De respectieve verantwoordelijkheden van Sciensano en van de overheden en agentschappen die bevoegd zijn inzake de uitoefening van de rechten van de betrokkene mogen niet bepaald worden door middel van een regeling die Sciensano, de deeltiteiten en de agentschappen onderling zouden sluiten. Een dergelijke tekst kan weliswaar nuttig zijn voor het harmoniseren en het coördineren van het beleid, maar de akkoorden die daarin vervat zijn, moeten worden omgezet in formele rechtsregels, temeer daar het net gaat om de uitoefening van de rechten van particulieren en het verstrekken van informatie ten behoeve van hen.

Artikel 17

42.1. Het volledige opschrift van de bijzondere wet van 8 augustus 1980 ‘tot hervorming der instellingen’ dient te worden vermeld.

42.2. De gemachtigden zijn het ermee eens dat het samenwerkingsakkoord overeenkomstig artikel 92bis, § 5, vierde en achtste lid, van de bijzondere wet van 8 augustus 1980, aangevuld dient te worden met een regeling van de wijze waarop de leden van het samenwerkingsgerecht, met uitzondering van de voorzitter, aangewezen worden en met een

regeling voor de werkingskosten van het samenwerkingsgerecht.⁶¹

Artikel 19

43. Overeenkomstig artikel 19, § 1, van het samenwerkingsakkoord heeft het uitwerking met ingang van 4 mei 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.⁶²

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 67.425/3-67.426/3-67.427/3 en 67.424/3, kan in die omstandigheden terugwerkende kracht worden verleend aan de bepalingen van het samenwerkingsakkoord die inhoudelijk overeenstemmen met hetgeen is geregeld in het koninklijk besluit nr. 18 van 4 mei 2020, met ingang van de datum van inwerkingtreding van dat besluit, namelijk 4 mei 2020.

Die verantwoording geldt echter niet voor nieuwe elementen die in het samenwerkingsakkoord werden toegevoegd in vergelijking met het koninklijk besluit nr. 18 van 4 mei 2020. Om die reden zou in artikel 19, § 1, van het samenwerkingsakkoord het best worden toegevoegd: “wat betreft de bepalingen die inhoudelijk overeenstemmen met het koninklijk besluit nr. 18 van 4 mei 2020 tot oprichting van een databank bij Sciensano in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19, zoals dat van toepassing was vanaf 4 mei 2020”.

Die verantwoording geldt evenmin voor artikel 14 van het samenwerkingsakkoord, dat betrekking heeft op de digitale contactopsporingsapplicaties, aangezien er nog geen dergelijke applicaties in gebruik zijn genomen en terugwerkende kracht hiervoor dus onnodig is. Dat artikel moet dan ook worden uitgezonderd van de terugwerkende kracht.

⁶¹ Zie Y. PEETERS, De plaats van samenwerkingsakkoorden in het constitutioneel kader, Brugge, die Keure, 2016, 329-330.

⁶² Vaste rechtspraak van het Grondwettelijk Hof, zie o.m.: GwH 21 november 2013, nr. 158/2013, B.24.2; GwH 19 december 2013, nr. 172/2013, B.22; GwH 29 januari 2014, nr. 18/2014, B.10; GwH 9 oktober 2014, nr. 146/2014, B.10.1; GwH 22 januari 2015, nr. 1/2015, B.4; GwH 7 mei 2015, nr. 54/2015, B.12; GwH 14 januari 2016, nr. 3/2016, B.22; GwH 3 februari 2016, nr. 16/2016, B.12.1; GwH 28 april 2016, nr. 58/2016, B.9.2; GwH 9 februari 2017, nr. 15/2017, B.9.2.

ONDERZOEK VAN HET VOORONTWERP VAN WET

44. Het opschrift van het voorontwerp en het artikel waarbij instemming verleend wordt aan het samenwerkingsakkoord dienen te worden aangevuld met de datum waarop het samenwerkingsakkoord is ondertekend.

45. Artikel 6 van het voorontwerp bevat een inwerkingtredingsbepaling. Een dergelijke bepaling in een instemmingstekst is zinloos en zelfs rechtsonzeker, nu de uitwerking in de tijd van het samenwerkingsakkoord in artikel 19, § 1, van dat samenwerkingsakkoord zelf wordt geregeld en het samenwerkingsakkoord niet vroeger in werking kan treden dan op de dag van bekendmaking van de laatst bekendgemaakte instemmingstekst.⁶³ Artikel 6 moet dan ook worden weggelaten.

*

⁶³ Y. PEETERS, *De plaats van samenwerkingsakkoorden in het constitutioneel kader*, o.c., 268-269.

1. Suivant l'article 84, § 1^{er}, alinéa 1^{er}, 3^o, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la demande d'avis doit spécialement indiquer les motifs qui en justifient le caractère urgent.

En l'espèce, l'urgence est motivée

“Het verzoek om spoedbehandeling is gemotiveerd door de omstandigheid dat dit voorontwerp betrekking heeft op een buitengewone crisissituatie, namelijk de gevolgen van de COVID-19-pandemie die momenteel in België heerst, wat bijzondere en ernstige problemen oplevert in termen van de volksgezondheid;

Dat het van vitaal belang is voor de volksgezondheid en voor het vermijden van een heropflakking van de COVID-19 pandemie, dat een gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams kan plaatsvinden met het oog op een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn, op basis van een gegevensbank bij Sciensano;

Dat de afdeling wetgeving in haar advies 67.425/3 over een wetsvoorstel 'tot oprichting van een databank bij Sciensano in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19' (Parl.St. Kamer 2019-20, nr. 55-1249/001) oordeelde dat de materie die het voorwerp uitmaakt van voornoemd wetsvoorstel, alsook van dit voorontwerp betrekking heeft zowel op federale als op gemeenschapsbevoegdheden, en de beoogde regelgeving enkel doorgang kan vinden indien ze zou worden omgevormd tot een samenwerkingsakkoord waarvoor parlementaire instemming is vereist;

Dat momenteel het bijzondere volmachtenbesluit nr. 44 van 26 juni 2020 omwille van de dringende noodzakelijkheid voorziet in een voorlopige regelgeving m.b.t. deze materie, in afwachting van een meer duurzame en rechtszekere oplossing onder de vorm van een samenwerkingsakkoord;

Dat het koninklijk besluit nr. 44 ophoudt uitwerking te hebben op 15 oktober 2020;

Dat het voor de goede werking, de continuïteit en het vertrouwen van de burger in het systeem van het contactonderzoek van belang is dat omtrent de beoogde gegevensverwerking zo snel mogelijk de nodig juridische zekerheid wordt gecreëerd;

Dat het bijgevolg van belang is dat dit samenwerkingsakkoord zo snel mogelijk en tegelijkertijd met de verschillende instemmingsakten gepubliceerd wordt in het Belgisch Staatsblad.”

*

2. Comme la demande d'avis est introduite sur la base de l'article 84, § 1^{er}, alinéa 1^{er}, 3^o, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet ¹, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

¹ S'agissant d'un avant-projet de loi, on entend par « fondement juridique » la conformité aux normes supérieures.

HISTORIQUE ET PORTÉE DE L'AVANT-PROJET DE LOI ET DE L'ACCORD DE COOPÉRATION

3. L'arrêté royal n° 18 du 4 mai 2020 'portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19' prévoyait la création d'une banque de données auprès de Sciensano² dans le cadre de la lutte contre le COVID-19 afin de recueillir des données de personnes testées au COVID-19 ou dont le diagnostic du COVID-19 a été confirmé, de personnes pour lesquelles il existe une présomption d'infection et de personnes avec lesquelles ces personnes ont été en contact. La durée de validité de cet arrêté – jusqu'au 4 juin 2020 – a été prolongée jusqu'au 30 juin 2020 par l'arrêté royal n° 25 du 28 mai 2020 'modifiant l'arrêté royal n° 18 du 4 mai 2020 portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19'. A suivi l'arrêté royal n° 44 du 26 juin 2020 'concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présümées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano', qui a reproduit telle quelle la substance du régime de l'arrêté royal n° 18 du 4 mai 2020 et qui est toujours en vigueur³. Aucun de ces arrêtés n'a été soumis à l'avis de la section de législation du Conseil d'État.

Le contenu de l'arrêté royal n° 18 du 4 mai 2020 a été quasi intégralement reproduit dans une proposition de loi 'portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19'⁴ qui, ainsi qu'un certain nombre d'amendements à celle-ci⁵, a été soumise au Conseil d'État pour avis. Dans l'avis n°s 67.425/3-67.426/3-67.427/3 du 26 mai 2020⁶, le Conseil d'État a constaté que la banque de données visée dans la proposition, le traitement des données à caractère personnel qui l'accompagne ainsi que les dispositions relatives aux missions et au fonctionnement du centre de contact portent sur le dépistage et la prévention d'infections au COVID-19. Dès lors, la proposition de loi se rapporte en grande partie à la compétence des communautés concernant le dépistage et la lutte contre les maladies contagieuses et sociales en tant que composante de leurs compétences en matière de médecine préventive⁷, de sorte que le Conseil d'État a recommandé

² Sciensano est une institution publique dotée de la personnalité juridique qui assume notamment un certain nombre de missions en matière de santé et de soutien à la politique de santé (voir les articles 3 et 4 de la loi du 25 février 2018 'portant création de Sciensano').

³ Conformément à son article 17 « [l'arrêté] cesse ses effets le jour où entre en vigueur un accord de coopération entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts des personnes (présümées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano » et au plus tard le 15 octobre 2020.

⁴ *Doc. parl.*, Chambre, 2019-2020, n° 55-1249/001.

⁵ *Ibidem*, n°s 55-1249/002 et 55-1249/003.

⁶ *Ibidem*, n° 55-1249/006.

⁷ Article 5, § 1^{er}, I, alinéa 1^{er}, 8°, de la loi spéciale du 8 août 1980 'de réformes institutionnelles'. Voir également *Doc. parl.*, Sénat, 1979-80, n° 434/2, p. 125 et *Doc. parl.*, Chambre, 1979-80, n° 627/10, p. 52. Cette compétence a été implicitement confirmée dans l'avis C.E. 34.339/AG du 29 avril 2003 sur un avant-projet devenu le décret de la Communauté flamande et de la Région flamande du 21 novembre 2003 'betreffende het preventieve

de transformer la proposition de loi en un accord de coopération pour lequel l'assentiment parlementaire est requis. Le Conseil d'État a réitéré cette conclusion dans l'avis n° 67.482/3 du 3 juin 2020⁸ sur un autre amendement⁹ à la même proposition de loi.

4. Une proposition de loi 'relative à l'utilisation d'applications numériques de traçage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population'¹⁰ a également été soumise à l'avis du Conseil d'État en même temps que la proposition de loi précitée. Le 26 mai 2020, le Conseil d'État a donné à ce sujet l'avis 67.424/3¹¹, dans lequel il a constaté que les applications numériques de traçage de contacts réglées dans la proposition et le traitement des données à caractère personnel y afférent se rapportent au dépistage et à la prévention des contaminations par le COVID-19. Dès lors, la proposition de loi se rapporte dans une large mesure à la compétence des communautés concernant le dépistage et la lutte contre les maladies contagieuses et sociales en tant que composante de leurs compétences en matière de médecine préventive. Dans ce cas également, le Conseil d'État a recommandé de transformer la proposition de loi en un accord de coopération pour lequel l'assentiment parlementaire est requis.

5. L'avant-projet de loi soumis pour avis a pour objet de porter assentiment à un accord de coopération qui remanie fondamentalement le dispositif contenu dans les deux propositions de loi précitées. Les parties à cet accord de coopération sont l'autorité fédérale, la Région wallonne, la Communauté flamande, la Communauté germanophone et la Commission communautaire commune.

5.1. L'accord de coopération crée auprès de Sciensano quatre bases de données (Bases de données I, III, IV et V), à côté de la base de données existante, dont les modalités sont définies au regard de la lutte contre le COVID-19 (Base de données II). L'article 1^{er}, § 1^{er}, 5° à 9°, de l'accord de coopération décrit ces cinq bases de données.

– La Base de données I est la base de données centrale générale créée auprès de Sciensano pour le traitement et l'échange de données aux fins de traitement fixées dans l'accord de coopération. Cette base de données centrale prévoit l'échange de données avec les bases de données créées pour soutenir les centres de contact des communautés.

– La Base de données II est la base de données existante auprès de Sciensano créée en exécution d'un accord de coopération conclu avec l'Institut national d'assurance maladie-invalidité (ci-après : INAMI) afin d'augmenter les connaissances épidémiologiques, cliniques et

gezondheidsbeleid', *Doc. parl.*, Parl. fl., 200203, n° 1709/1, pp.147-155, ainsi que expressément dans les avis C.E. 38.381/3 du 7 juillet 2005 sur un projet d'arrêté royal 'établissant les mesures prophylactiques et la déclaration obligatoire à la cellule de vigilance sanitaire de pathologies présentant un caractère épidémique' et C.E. 53.018/VR du 13 mai 2013 sur un projet d'arrêté royal 'relatif au contrôle sanitaire du trafic international'.

⁸ *Doc. parl.*, Chambre, 2019-2020, n° 55-1249/009.

⁹ *Ibidem*, n° 55-1249/004.

¹⁰ *Doc. parl.*, Chambre, 2019-2020, n° 55-1251/001.

¹¹ *Ibidem*, n° 55-1251/003.

autres¹². Les données, fournies dans le cadre du suivi manuel des contacts, doivent permettre aux institutions de recherche, dont Sciensano, d'effectuer des études scientifiques ou statistiques en rapport avec la propagation du coronavirus COVID-19 et de soutenir la politique de lutte contre le coronavirus par l'échange des données avec la Base de données I.

– La Base de données III est la base de données des demandes d'appel et des demandes pour le personnel du centre de contact.

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

– La Base de données V est le journal central des enregistrements qui permet de contrôler le fonctionnement de l'application numérique de traçage des contacts et qui, au sein de Sciensano, est séparée des Bases de données I et II. Une application numérique de traçage des contacts sur la base du DP3T¹³ se compose en effet d'une application mobile qui peut être, sur une base volontaire, installée et utilisée par l'utilisateur en local sur son appareil, et d'un journal central des enregistrements conservé dans la Base de données V.

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

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

¹² Voir l'article 22, 20°, de la loi 'relative à l'assurance obligatoire soins de santé et indemnités', coordonnée le 14 juillet 1994, ajouté par la loi du 10 avril 2014.

¹³ DP3T est l'abréviation du protocole ouvert « Decentralised Privacy-Preserving Proximity Tracing » (voir https://en.wikipedia.org/wiki/Decentralized_Privacy-Preserving_Proximity_Tracing).

Le chapitre III contient l'article 4, qui définit les catégories de personnes dont les données à caractère personnel sont traitées dans le cadre de l'accord de coopération à l'examen. Ces catégories sont définies à l'article 1^{er}, § 1^{er}, 12^o à 17^o.

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

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

– Personnes de catégorie III : les personnes que le médecin soupçonne sérieusement d'être infectées, sans qu'un test de dépistage du COVID-19 ait été effectué ou prescrit, ou dont le test de dépistage du COVID-19 a révélé qu'elles n'étaient pas infectées ;

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

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

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

Le chapitre IV détermine les catégories de données à caractère personnel qui sont traitées dans le cadre de l'accord de coopération. L'article 5 prescrit que le traitement des données doit être effectué conformément au RGPD¹⁴ et à la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel'. L'article 6 requiert que les déclarations obligatoires en vertu de la réglementation communautaire soient faites auprès de la Base de données I (paragraphe 1^{er}) et définit les catégories de données à caractère personnel qui sont traitées dans cette base de données, respectivement, pour les Personnes de catégorie I, les Personnes de catégorie II, les Personnes de catégorie III et les Personnes de catégorie IV (paragraphe 2 à 5). Les paragraphes 6 et 7 définissent les données à caractère personnel supplémentaires à traiter pour certaines catégories de personnes et de clusters, qui sont collectées ou fournies par les équipes mobiles ou les inspections d'hygiène compétentes. L'article 7 définit les catégories de données à caractère personnel qui sont traitées dans la Base de données III, à savoir les données à caractère personnel qui sont communiquées par Sciensano à partir de la Base de données I aux centres de contact (paragraphe 1^{er}), les données à caractère personnel pour la Base de données III en ce qui concerne les Personnes de catégorie II qui, après avoir effectué un test de dépistage du COVID-19, se sont avérées infectées, et les Personnes de catégorie III (paragraphe 2), les Personnes de catégorie IV (paragraphe 3) et les Personnes de

¹⁴ 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)'.

catégorie VI (paragraphe 4). L'article 8 définit les catégories de données à caractère personnel qui sont traitées dans la Base de données IV en ce qui concerne les Personnes de catégorie V et de catégorie VI. L'article 9 définit les catégories de données à caractère personnel qui, après pseudonymisation, sont traitées dans la Base de données II en ce qui concerne les Personnes de catégorie I, de catégorie II et de catégorie III (paragraphe 1^{er}) et les Personnes de catégorie IV (paragraphe 2).

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

Le chapitre VI concerne la compétence du Comité de sécurité de l'information ¹⁵. L'article 11 règle la délibération préalable, dans certains cas, au sein de ce comité (paragraphe 1^{er} et 2) et la compétence de ce comité de préciser des données (paragraphe 3). Il est également prévu de régler certains aspects de l'accord de coopération dans un accord de coopération d'exécution (paragraphe 4). L'article 12 définit les modalités que le Comité de sécurité de l'information peut fixer (paragraphe 1^{er}) et règle l'accès au Registre national et aux registres de la Banque-carrefour de la sécurité sociale (paragraphe 2), ainsi que la délibération préalable au sein du Comité de sécurité de l'information pour la communication de données à caractère personnel provenant d'autres sources authentiques que la Base de données I (paragraphe 3).

Le chapitre VII contient l'article 13, qui concerne les mesures de sécurité que Sciensano doit prendre afin de garantir un niveau de sécurité adapté au risque.

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

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

Le chapitre X concerne la transparence et les droits des personnes concernées. L'article 16 énonce l'obligation pour Sciensano en tant que responsable du traitement de prendre

¹⁵ Créé par 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'.

des mesures appropriées en matière de communication des droits des personnes concernées (paragraphe 1^{er}), créer et à assurer la maintenance d'un site internet (paragraphe 2), gérer et assurer la maintenance d'un système pour l'exercice des droits prévus dans le RGPD (paragraphe 3) et conclure un accord avec les autorités compétentes et leurs agences en ce qui concerne leurs responsabilités en matière d'exercice des droits des personnes concernées et la fourniture d'informations (paragraphe 4).

Le chapitre VIII (lire : XI) contient diverses dispositions finales. L'article 17 organise le règlement des litiges entre les parties par une juridiction de coopération. L'article 18 charge la Conférence interministérielle Santé publique de surveiller la mise en œuvre et le respect des dispositions de l'accord de coopération, et de proposer des adaptations. L'article 19 règle l'entrée en vigueur rétroactive de l'accord de coopération (paragraphe 1^{er}) et prévoit la possibilité de sa résiliation par un nouvel accord de coopération (paragraphe 2).

COMPÉTENCE

6. Ainsi qu'il a déjà été exposé dans les observations 3 et 4, les avis n^{os} 67.425/3-67.426/3-67.427/3 et n^o 67.424/3 avaient conclu à la nécessité de conclure un accord de coopération entre l'autorité fédérale et les communautés pour les dispositifs visés en matière de traitement des données à caractère personnel relatifs au traçage manuel et numérique des contacts. Même si l'accord de coopération auquel on entend porter assentiment remanie en profondeur le contenu des deux propositions de loi qui ont fait l'objet de ces avis, la conclusion reste cependant identique en ce qui concerne les compétences, et ce sous réserve de ce qui suit.

6.1. Par le décret spécial du 3 avril 2014 et les décrets des 4 et 11 avril 2014 'relatif[s] aux compétences de la Communauté française dont l'exercice est transféré à la Région wallonne et à la Commission communautaire française', la Communauté française, la Commission communautaire française et la Région wallonne ont respectivement décidé d'un commun accord, conformément à l'article 138 de la Constitution, que la Région wallonne et la Commission communautaire française exercent, notamment, la compétence de la Communauté française en matière de politique de santé, visée à l'article 5, § 1^{er}, I, de la loi spéciale du 8 août 1980 'de réformes institutionnelles', dont la compétence communautaire en matière d'établissements de soins, y compris les hôpitaux (à l'exception des hôpitaux universitaires) et en matière de médecine préventive (à l'exception notamment « des activités et services de médecine préventive destinés aux nourrissons, aux enfants, aux élèves et aux étudiants » et « de ce qui relève des missions confiées à l'Office de la Naissance et de l'Enfance (ONE) »)¹⁶.

Dans la mesure où la réglementation inscrite dans l'accord de coopération comporte également des obligations pour les établissements de soins, parmi lesquels les hôpitaux¹⁷, il s'impose qu'outre les parties actuelles à l'accord de coopération, la Communauté française et la Commission communautaire française y soient également associées en tant que parties.

¹⁶ Article 3, 6^o, des décrets précités.

¹⁷ Voir les articles 2, § 1^{er}, et 6, § 3, alinéa 2, de l'accord de coopération.

La Communauté française a en effet conservé l'exercice de sa compétence de principe pour imposer des obligations aux hôpitaux universitaires établis dans la région de langue française et aux hôpitaux universitaires établis dans la région bilingue de Bruxelles-Capitale qui, en raison de leur organisation, doivent être considérés comme appartenant exclusivement à la Communauté française ¹⁸.

Pour sa part, la Commission communautaire française exerce la compétence de principe pour imposer des obligations aux hôpitaux privés établis dans la région bilingue de Bruxelles-Capitale qui, en raison de leur organisation, doivent être considérés comme appartenant exclusivement à la Communauté française ¹⁹.

À ce sujet, les délégués ²⁰ ont déclaré ce qui suit :

« [T]ijdens verschillende [interkabinettenwerkgroepen] heeft de Franse Gemeenschapscommissie zelf aangegeven dit deel van hun bevoegdheid door middel van de Gemeenschappelijke Gemeenschapscommissie te willen regelen. Hierdoor is de Franse Gemeenschapscommissie uiteindelijk geen partij meer bij het samenwerkingsakkoord, maar wordt zij vertegenwoordigd door de Gemeenschappelijke Gemeenschapscommissie ».

Les règles répartitrices de compétences sont des règles de droit contraignantes d'ordre public qui ne se prêtent pas à des mécanismes, tels que la renonciation ou la représentation par accord mutuel entre autorités. Il faut dès lors en conclure qu'il y a lieu d'appeler tant la Communauté française que la Commission communautaire française à être parties à l'accord de coopération. S'il en résulte que des adaptations de fond sont apportées à la réglementation portée par l'accord de coopération, les avant-projets de textes d'assentiment à l'accord de coopération adapté devront à nouveau être soumis pour avis au Conseil d'État.

6.2. Tant l'intitulé que le dispositif de l'accord de coopération font systématiquement référence aux « autorités régionales ». L'expression « autorités régionales » ne permet toutefois pas de désigner valablement les autorités communautaires qui sont (ou sont appelées) à être parties à l'accord de coopération. Il convient dès lors d'omettre le mot « régionales » de l'intitulé et du dispositif de l'accord de coopération.

FORMALITÉS PRÉALABLES

7.1. L'article 14 de l'accord de coopération, qui concerne les applications de traçage numérique des contacts, comporte un certain nombre de règles techniques au sens de l'article premier, paragraphe 1, f), de la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 'prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information', et

¹⁸ Voir l'article 128, § 2, de la Constitution, ainsi que l'article 3, 6°, des décrets précités.

¹⁹ Voir l'article 128, § 2, de la Constitution, ainsi que l'article 3, 6°, des décrets précités.

²⁰ La mention « les délégués » vise ici (et également dans la suite du présent avis) les délégués qui ont été désignés dans la demande d'avis sur l'avant-projet de loi d'assentiment, qui a donné lieu à l'avis n° 67.719/VR.

plus particulièrement des règles relatives aux services de la société de l'information au sens de l'article premier, paragraphe 1, e), de cette directive.

Conformément à l'article 5 de la directive (UE) 2015/1535, de telles règles techniques doivent être notifiées à la Commission européenne. Dans ce cas, un délai d'attente de trois mois (au moins) s'applique avant que la proposition de loi puisse être adoptée, conformément à l'article 6 de la directive. Toutefois, conformément à l'article 6, paragraphe 7, ce délai d'attente ne s'applique pas lorsqu'un État membre, pour des raisons urgentes tenant à une situation grave et imprévisible qui a trait à la protection (notamment) de la santé des personnes, doit élaborer à très bref délai des règles techniques pour les arrêter et les mettre en vigueur aussitôt, sans qu'une consultation soit possible. Dans ce cas, la communication à la Commission est toujours requise; la communication doit mentionner le motif qui justifie l'urgence. La Commission se prononce ensuite sur la communication dans les plus brefs délais.

Par conséquent, la proposition doit être notifiée à la Commission européenne, l'urgence de son adoption pouvant alors être exposée pour justifier le non-respect du délai d'attente prescrit ²¹.

7.2. La question se pose en outre de savoir si l'article 14 de l'accord de coopération relève du champ d'application de la directive « services » ²². La mise à disposition d'une application numérique de traçage de contacts doit être considérée comme un service qui peut éventuellement être fourni contre rémunération, que cette rémunération émane de l'autorité ou – éventuellement par voie de recettes publicitaires – de l'utilisateur. L'accord de coopération ne garantit nullement que les applications sont proposées en tant que service non économique d'intérêt général ²³. L'exception pour les services de soins de santé ²⁴ ne peut non plus être invoquée, dès lors que les applications ne concernent pas des activités réservées à une profession de santé réglementée dans l'État membre où le service est fourni ²⁵.

Il est dès lors possible que la directive « services » s'applique ²⁶, de sorte que la disposition précitée de l'accord de coopération doit être examinée au regard des articles 14 et 15 de cette directive en ce qui concerne les exigences prévues pour l'exercice d'une activité de service sur le territoire de la Belgique ²⁷. À première vue, l'accord de coopération ne semble pas contenir d'exigences interdites au sens de cet article 14, ni d'exigences non discriminatoires au sens de cet article 15, paragraphe 2. Le Conseil d'État ne dispose toutefois pas des connaissances techniques requises concernant les exigences spécifiques relatives aux applications numériques

²¹ Voir dans le même sens l'avis n° 67.424/3, observation 10.

²² Directive n° 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 'relative aux services dans le marché intérieur'.

²³ Voir l'article 2, paragraphe 2, a), de la directive « services ».

²⁴ Voir l'article 2, paragraphe 2, f), de la directive « services ».

²⁵ *Manuel relatif à la mise en œuvre de la directive « services »*, Commission européenne, 2007, p. 12. Voir également le considérant 22 de la directive « services ».

²⁶ Les motifs d'exception prévus à l'article 2, paragraphe 2, c) et i), ne semblent en tout cas pas non plus s'appliquer en l'espèce.

²⁷ Puisqu'un régime d'autorisation n'est en effet pas prévu, il n'y a pas lieu d'effectuer un contrôle au regard des articles 9 à 13 de la directive « services ».

de traçage de contacts pour pouvoir apprécier ce point de manière concluante. Le cas échéant, une notification à la Commission européenne, conformément à l'article 15, paragraphe 7, de la directive « services » pourrait être néanmoins encore requise ²⁸.

EXAMEN DE L'ACCORD DE COOPÉRATION

OBSERVATIONS GÉNÉRALES

A. Version allemande authentique de l'accord de coopération

8. Il n'existe pas encore de version allemande authentique de l'accord de coopération signée par toutes les parties. Les délégués ont déclaré que cette version était encore en préparation au moment où la demande d'avis a été introduite. Les versions authentiques en français et en néerlandais de l'accord de coopération ayant été signées, notamment, par le Ministre-Président et le ministre compétent de la Communauté germanophone, et compte tenu de l'urgence de la réglementation contenue dans l'accord de coopération, le Conseil d'État peut exceptionnellement admettre que l'absence de la version allemande authentique de l'accord de coopération ne porte pas atteinte à la recevabilité de la demande d'avis.

B. Compatibilité avec la norme supérieure en matière de protection des données à caractère personnel

9. L'accord de coopération à l'examen envisage des traitements de données à caractère personnel qui constituent des ingérences dans le droit au respect de la vie privée des personnes concernées, garanti notamment par l'article 22 de la Constitution et l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après : CEDH).

Pour être admissible au regard des dispositions précitées, l'ingérence dans l'exercice du droit au respect de la vie privée doit être 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. Toute ingérence dans le droit au respect de la vie privée doit, en outre, reposer sur une justification raisonnable et être proportionnée aux buts poursuivis par le législateur ²⁹.

Si les ingérences prévues par l'accord de coopération à l'examen poursuivent un objectif légitime, à savoir la protection de la santé ainsi que la protection des droits et libertés

²⁸ Voir dans le même sens l'avis n° 67.424/3, observation 11.

²⁹ Avis n° 63.192/2 donné le 19 avril 2018 sur l'avant-projet devenu la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel', *Doc. parl.*, Chambre, 2017-2018, n° 54-3126/1, pp. 402 à 456, <http://www.raadvst-consetat.be/dbx/avis/63192.pdf> ; avis n° 63.202/2 donné le 28 avril 2018 sur l'avant-projet devenu 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', *Doc. parl.*, Chambre, 2017-2018, n° 54-3185/1, pp. 120 à 145, <http://www.raadvst-consetat.be/dbx/avis/63202.pdf>.

d'autrui³⁰, il convient de vérifier le respect des exigences de légalité, de pertinence et de proportionnalité tant pour le traçage manuel que pour le traçage numérique des contacts que règle l'accord de coopération.

1. Le principe de légalité inscrit à l'article 22 de la Constitution

10.1. Conformément à l'article 22 de la Constitution, tout traitement de données à caractère personnel et, plus généralement, toute atteinte au droit à la vie privée, sont soumis au respect d'un principe de légalité.

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, l'article 22 de la Constitution garantit 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 porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur³¹.

10.2. Par conséquent, les éléments essentiels des traitements de données à caractère personnel doivent être fixés dans la loi elle-même³².

10.3. Le principe de légalité en matière de traitement des données à caractère personnel s'oppose à une définition trop vague des éléments essentiels du régime en la matière figurant dans l'accord de coopération.

Un certain nombre de dispositions de l'accord de coopération font état de données qui sont « nécessaires » pour établir le contact avec les personnes qui y sont mentionnées³³ ou d'informations ou de critères qui sont « pertinent(e)s » pour certaines situations³⁴. Compte tenu notamment de l'importance d'un fonctionnement rapide et adéquat du traçage des contacts et du traitement des données y afférent, il peut être admis que les données concernées ne soient pas énumérées de manière exhaustive dans l'accord de coopération même.

L'article 9, § 1^{er}, 13°, de l'accord de coopération fait mention des « données communiquées au centre de contact, en ce compris les symptômes, la date des premiers symptômes, les déplacements, le suivi des mesures d'isolement et d'hygiène ». Une telle définition des données à traiter, qui implique que toutes les données communiquées peuvent faire

³⁰ Article 8, § 2, de la CEDH.

³¹ Jurisprudence constante de la Cour constitutionnelle : voir notamment C.C., 18 mars 2010, n° 29/2010, B.16.1 ; C.C., 20 février 2020, n° 27/2020, B.17.

³² Voir notamment l'avis n° 64.879/4 donné le 4 février 2019 sur un avant-projet devenu le décret de la Région wallonne du 2 mai 2019 'modifiant le Code wallon de l'action sociale et de la santé en ce qui concerne la prévention et la promotion de la santé' *Doc. parl.*, Parl. wall., 2018-2019, n° 1332/1, pp. 25 à 35, <http://www.raadvst-consetat.be/dbx/avis/64879.pdf> et l'avis n° 66.443/1/V donné le 29 août 2019 sur un projet devenu l'arrêté royal du 9 février 2020 'relatif à l'enregistrement des déclarations de volonté concernant le prélèvement de matériel corporel humain, y compris les organes, après le décès', <http://www.raadvst-consetat.be/dbx/avis/66443.pdf>.

³³ Voir l'article 6, § 4, 12°, et § 5, 7°, l'article 7, § 2, 6°, et § 3, 7°, l'article 9, § 2, 8°, et l'article 14, § 4, alinéa 2, de l'accord de coopération.

³⁴ Voir l'article 6, § 5, 9° et 10°, l'article 7, § 3, 9° et 10°, et l'article 9, § 2, 9°, de l'accord de coopération.

l'objet d'un traitement, est trop large et doit être expressément limitée aux données qui sont pertinentes pour le traçage des contacts. La circonstance que ces données sont pseudonymisées³⁵ ne change rien à cette constatation.

10.4.1. Certaines délégations contenues dans l'accord de coopération à l'examen concernent des éléments essentiels dont le règlement est réservé au législateur par l'article 22 de la Constitution.

Tel est en particulier le cas :

– de l'habilitation contenue à l'article 11, § 4, de l'accord de coopération, dans la mesure où elle délègue la compétence de « modifier ou compléter les catégories de données à caractère personnel traitées dans les bases de données » ;

– des articles 11, § 3, et 12, § 1^{er}, de l'accord de coopération qui habilite la Chambre « Sécurité sociale et Santé » du Comité de la sécurité de l'information, à définir et préciser les données à caractère personnel spécifiques pouvant être traitées et communiquées, pour chaque finalité de traitement, ainsi que les modalités en la matière³⁶.

En effet, comme la section de législation l'a déjà fait observer dans son avis n^{os} 67.425/3-67.426/3-67.427/3 :

« Dans la mesure où les délégations proposées se rapportent à des catégories supplémentaires de données à caractère personnel ou à des finalités supplémentaires de traitement de telles données, les catégories et finalités visées doivent être réglées dans le texte de la proposition et elles ne peuvent pas être déléguées par le législateur. Par contre, s'il s'agit uniquement de poursuivre la concrétisation de catégories et de finalités déjà définies dans la proposition, ladite concrétisation peut être déléguée³⁷ ».

L'accord de coopération sera revu en conséquence.

10.4.2. En outre, certains aspects de la délégation faite par l'article 14, § 9, de l'accord de coopération à un accord de coopération d'exécution pour ce qui concerne les modalités de fonctionnement de l'application numérique de traçage des contacts touchent également à des éléments essentiels devant être réglés par le législateur conformément à l'article 22 de la Constitution.

Ainsi, des éléments comme la description des traitements résultant de l'utilisation de l'application numérique de traçage des contacts (§ 9, 2^o), les modes d'information des utilisateurs (§ 9, 6^o) et la procédure de contrôle (§ 9, 7^o) devraient être mieux encadrés dans l'accord de coopération à l'examen.

L'accord de coopération sera par conséquent adapté et complété à cet égard.

³⁵ Voir l'article 9, § 1^{er}, phrase introductive, de l'accord de coopération.

³⁶ Voir par ailleurs l'observation particulière sous les articles 11 et 12.

³⁷ *Note de bas de page n° 15 de l'avis cité* : Comparer avec C.C., 4 avril 2019, n° 49/2019, B.46.7 et B.47.2.

2. Le principe de minimisation des données

11.1. Conformément à l'article 5, paragraphe 1, c), du RGPD, les données à caractère personnel qui font l'objet d'un traitement sont « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». Selon l'Autorité de protection des données, il est porté atteinte à ce principe de minimisation des données par la « centralisation d'une quantité importante de données relatives à la santé dans une banque de données unique constituée, détenue et gérée par un acteur qui ne ferait office que d'intermédiaire »³⁸. Le délégué justifie le choix de la centralisation des données à caractère personnel dans la Base de données I centrale comme suit :

« De organisatie van de gegevensbanken is gebaseerd op principes van data protection by design, data protection by default en dataminimalisatie. Meervoudige opslag van dezelfde persoonsgegevens in gegevensbanken bij verschillende gefedereerde entiteiten is vermeden.

ICT-technisch heeft elke gegevensbank uiteraard een eigen onderliggend gegevensmodel. Verschillende gegevensmodellen geven aanleiding tot verschillende gegevensbanken. Zowel de GBA als de Raad van State hebben verzocht om het gegevensmodel van de onderscheiden gegevensbanken in detail te beschrijven, wat in het ontwerp van samenwerkingsakkoord is gebeurd.

Gegevensbank I is noodzakelijkerwijze een gemeenschappelijke gegevensbank over de gefedereerde entiteiten heen omdat het opvolgen van de contacten zich niet kan beperken tot de personen die ressorteren onder één deelstaat. Het organiseren van een gegevensbank per gefedereerde entiteit zou ertoe leiden dat elk gewest of een gemeenschap een eigen duplicaat van de gehele gegevensbank moet beheren, en er permanente synchronisatie zou moeten geschieden met het risico op datalekken. Dat is in strijd met principes van dataminimalisatie en informatieveiligheid voorzien in de AVG.

Daarenboven zou organiseren van een gegevensbank per gefedereerde entiteiten fundamentele, negatieve impact hebben op de omlooptijd binnen het gehele manuele contactonderzoek. Immers, de verschillende bewerkingen om de uitwisselingen van gegevens tussen de verschillende databanken van de deelstaten te organiseren, zou dermate veel tijd innemen dat dit het hele proces zou vertragen (van het opvolgen van personen die een test dienen te ondergaan tot het contacteren van de Personen Categorie II voor zover de test uitwees dat ze besmet zijn en Personen Categorie III).

De Gegevensbank III is een afzonderlijke gegevensbank die enkel de (bel)orders bevat voor de medewerkers van de contactcenters. Deze gegevensbank heeft een ander gegevensmodel dan Gegevensbank I en is dus een afzonderlijke gegevensbank. Overigens is een scheiding tussen Gegevensbank I en Gegevensbank III een maatregel van data protection by design om te vermijden dat de medewerkers van het contact center onnodige toegang zouden kunnen hebben tot de gezondheidsgegevens in Gegevensbank I. De Gegevensbank III is een gemeenschappelijke gegevensbank over de contact centers heen om dezelfde reden als gegevensbank I een gemeenschappelijke gegevensbank is over de gefedereerde entiteiten heen.

Gegevensbank IV is een afzonderlijke gegevensbank die informatie bevat over de contactpersonen van te contacteren collectiviteiten. Deze Gegevensbank heeft een ander gegevensmodel dan Gegevensbank I en Gegevensbank III en is dus een afzonderlijke gegevensbank ».

³⁸ Avis n° 42/2020 de l'Autorité de protection des données du 25 mai 2020, observation 3.

Il est recommandé de faire figurer cette justification dans le commentaire général de l'avant-projet de texte d'assentiment.

11.2. Par rapport aux arrêtés royaux et à la proposition de loi mentionnés dans l'observation 3, l'accord de coopération énumère davantage de données à caractère personnel à traiter. À cet égard, les délégués ont donné la justification suivante :

« Men heeft hier willen voldoen aan een opmerking van de GBA. De GBA was bezorgd omdat het niet duidelijk was welke concrete persoonsgegevens werden gevraagd. Omwille van deze reden, werd naast het olijsten van de categorieën van persoonsgegevens (hetgeen onder de AVG zou moeten volstaan) ook reeds voorzien in een olijsting van de persoonsgegevens die onder een bepaalde categorie vallen. Het samenwerkingsakkoord gaat in de praktijk aldus niet verder dan initieel voorzien in het KB nr. 18. Er is wel sprake van een meer gedetailleerde beschrijving van de werkelijke gang van zaken. Dit teneinde tegemoet te komen aan de transparantievereiste van de AVG ».

À première vue, il peut être admis que les données à caractère personnel ajoutées sont, elles aussi, conformes au principe de minimisation des données.

11.3. Ainsi qu'il ressort du commentaire général et du dispositif de l'accord de coopération, le traçage numérique des contacts n'a pas vocation à remplacer le suivi manuel, mais bien à le compléter. Par conséquent, vu le traitement à grande échelle des données qui accompagne l'utilisation de l'application numérique de traçage, il convient d'être en mesure d'en démontrer la conformité au principe de minimisation des données.

Dans son avis 67.424/3, le Conseil d'État a déjà observé qu'eu égard au caractère volontaire des applications numériques de traçage de contacts, leur efficacité dépendra d'un taux de couverture suffisamment élevé, en d'autres termes du nombre de citoyens qui utiliseront l'application³⁹. Ce taux de couverture déterminera la mesure dans laquelle les applications pourront effectivement jouer un rôle complémentaire, à côté du traçage manuel de contacts mis en œuvre par les autorités compétentes. Par ailleurs, il y a également lieu de tenir compte du traitement à grande échelle de données à caractère personnel accompagnant l'utilisation de ces applications. En effet, conformément au principe de minimisation des données, ce traitement doit être limité à ce qui est nécessaire pour atteindre les objectifs visés. Il importe donc de concilier ce principe de nécessité avec un taux de couverture suffisamment élevé.

À cet égard, il faut également relever l'analyse d'impact relative à la protection des données que le responsable du traitement doit effectuer avant le début des opérations de traitement, conformément à l'article 35 du RGPD, « [l]orsqu'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 ». Tel est également le cas en l'espèce⁴⁰, comme le confirme d'ailleurs

³⁹ Voir <https://ukhumanrightsblog.com/2020/05/01/what-are-the-data-privacy-considerations-of-contact-tracing-apps/>.

⁴⁰ Voir en ce sens également l'avis n° 34/2020 du 28 avril 2020 de l'Autorité de protection des données, observations 23 et 48.

l'article 14, § 8, de l'accord de coopération, de sorte que cette analyse d'impact devra de toute façon être effectuée, de préférence préalablement à l'assentiment parlementaire.

Contrairement à la proposition de loi citée dans l'observation 4, l'accord de coopération ne prévoit pas d'évaluation de la réglementation portée par l'accord de coopération lui-même. L'avis 67.424/3 a souligné l'importance d'une telle évaluation, « [d]ès lors qu'il s'agit en l'occurrence d'une nouvelle technologie et eu égard à l'importance d'un suivi minutieux de la mise en balance précitée entre un taux de couverture suffisamment élevé et le principe de nécessité du traitement de données à caractère personnel accompagnant les applications ». Les délégués ont justifié l'absence d'une telle obligation d'évaluation dans l'accord de coopération comme suit :

« Aangezien het samenwerkingsakkoord slechts een algemeen kader voorziet voor de contactopsporingsapplicatie, dat dan verder door de deelstaten moet ingevuld worden, is een vorm van evaluatie niet aan de orde. De evaluatie zal immers moeten plaatsvinden op het niveau van de deelstaten. Gelieve te willen noteren dat na deze crisis een evaluatie van de gehele aanpak van deze crisis zal gebeuren, derhalve ook van het proces van het manuele contactonderzoek tot het inzetten van een digitale contactopsporingsapplicatie ».

11.4. Par ailleurs, au regard du respect du principe minimisation des données, se pose la question de savoir comment assurer le respect de la réglementation en matière de traçage numérique des contacts. L'accord de coopération à l'examen se contente de déléguer à un accord de coopération d'exécution le soin de prévoir « la procédure de contrôle du bon fonctionnement de l'application de traçage des contacts »⁴¹. À cet égard, la section de législation a déjà fait observer que : « Mieux vaut sans doute prévoir des sanctions administratives ou pénales pour la mise à disposition d'applications non conformes »⁴².

11.5. La question de la fin du traçage numérique des contacts se pose également au regard du respect du principe de minimisation des données.

À cet égard, l'article 14, § 3, 10°, de l'accord de coopération dispose que

« Le journal central des enregistrements de la Base de données V est en tout cas désactivé dès qu'il est établi par un accord de coopération d'exécution visé à l'article 92*bis*, § 1^{er}, troisième alinéa de la loi spéciale du 8 août 1980 de réformes institutionnelles que ces enregistrements ne sont plus nécessaires pour gérer la fin de la stratégie de déconfinement ; le journal central des enregistrements est désactivé automatiquement au plus tard après 1 an, sauf s'il est décidé par un accord de coopération d'exécution qu'une prolongation de cette période est indispensable ».

Les auteurs de l'accord de coopération doivent être en mesure d'expliquer pourquoi la désactivation prévue ne concerne que le journal central des enregistrements et non l'application numérique de traçage des contacts dans son entièreté.

⁴¹ Article 14, § 9, 7°, de l'accord de coopération.

⁴² Avis n° 67.424/3, observation 15.2.

De manière plus générale, afin de satisfaire à l'exigence de proportionnalité, il convient de prévoir une fin de validité précise pour l'ensemble des mesures prévues par l'accord de coopération ⁴³.

3. Le principe d'intégrité et de confidentialité

12. Le respect du principe d'intégrité et de confidentialité (article 5, paragraphe 1, f), du RGPD) exige enfin que des garanties suffisantes soient mises en place pour prévenir tout abus de cette ingérence dans la vie privée.

L'accord de coopération contient plusieurs garanties pour éviter tout abus, telles la publication du code source, l'utilisation volontaire de l'application numérique, l'absence de désavantage en cas de non-utilisation de celle-ci et la non-identification des utilisateurs.

La question se pose toutefois de savoir si ces différentes garanties sont suffisantes pour prévenir tout abus et limiter autant que possible l'ingérence.

L'accord de coopération impose le recours au protocole « DP3T ». Le commentaire général indique que ce système « devrait permettre de minimiser l'ingérence dans la sphère privée ». Comme le souligne l'Autorité de protection des données, il conviendrait toutefois de compléter ce commentaire par des explications quant aux « composantes essentielles du protocole DP3T, des garanties qu'il offre, des risques subsistant et des raisons pour lesquelles il faut conclure au caractère néanmoins proportionné des traitements de données qui seraient effectués » ⁴⁴.

Outre les difficultés que le procédé soulève au regard du principe de légalité⁴⁵, la section de législation relève que l'accord de coopération laisse à un futur accord de coopération d'exécution le soin de définir diverses garanties : la description du système de traçage, les définitions des concepts importants tels que le contact à risque, le code d'autorisation, la clé sécurisée et le numéro de série temporaire non personnalisé ⁴⁶, les garanties spécifiques pour limiter le risque de réidentification et la manière dont les personnes seront informées du fonctionnement de l'application numérique et la procédure de contrôle du bon fonctionnement de celle-ci (article 14, § 9, de l'accord de coopération à l'examen).

⁴³ Voir l'observation particulière sous l'article 19.

⁴⁴ Avis n° 43/2020, p. 16.

⁴⁵ Voir ci-avant l'observation relative au respect du principe de légalité.

⁴⁶ À cet égard, l'Autorité de protection des données a également fait remarquer que « [p]ar ailleurs, le principe de minimisation du RGPD implique de ne traiter que des données strictement nécessaires et pertinentes pour la finalité poursuivie. Dès lors, au vu de la définition des contacts à haut risque déterminée par le SPF Santé publique et le Centre de crise (contact de moins de 1,5 mètres avec une personne contaminée pendant plus de 15 minutes), l'Autorité considère que seuls ces contacts (le cas échéant avec une marge d'erreur acceptable du type « contact de moins de 4 mètres de distance pendant plus de 10 minutes ») doivent être captés (d'autant plus que la technologie Bluetooth permet de capter les contacts jusqu'à 100 mètres, ce qui est manifestement disproportionné pour la finalité poursuivie). La rédaction de la finalité devra être revue sur cette base et une définition de la notion de « contact à risque » conforme aux recommandations officielles sera utilement intégrée à l'article 3 de la proposition de loi par souci de sécurité juridique » (avis n° 43/2020, point 27).

Il s'ensuit que la section de législation n'est pas en mesure d'évaluer à ce stade si des garanties suffisantes existeront pour éviter tout abus lors de l'utilisation des applications numériques de traçage des contacts.

C. Correspondance entre les textes français et néerlandais de l'accord de coopération

13. Le texte de l'accord de coopération contient de nombreuses négligences sur le plan linguistique. L'accord de coopération doit dès lors encore faire l'objet d'un contrôle approfondi sur le plan de la rédaction et de la correction de la langue, en particulier en ce qui concerne la correspondance entre les textes français et néerlandais.

À titre d'exemple, on peut relever ce qui suit :

– dans le texte français de l'article 2, § 5, de l'accord de coopération, on remplacera chaque fois la mention « 41ompétente sou » par « compétentes ou » ;

– à la fin du texte néerlandais de l'article 3, § 1^{er}, 3^o, de l'accord de coopération, on visera l'article 10, § 2, au lieu de l'article 11, § 2 ;

– dans le texte néerlandais de l'article 10, § 3, de l'accord de coopération, il convient d'écrire « Gegevensbank I » au lieu de « Gegevensbank ».

OBSERVATIONS PARTICULIÈRES

PRÉAMBULE

14. Dès lors qu'il est étranger au fondement juridique de l'accord de coopération, l'alinéa 3 sera omis ou déplacé sous la forme d'un considérant.

15. L'alinéa 10 sera omis dès lors qu'il est redondant avec l'alinéa 4.

16. L'alinéa 15 sera omis dès lors que l'arrêté royal n° 18 du 4 mai 2020 'portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19' a cessé de produire ses effets le 30 juin 2020.

DISPOSITIF

Article 1^{er}

17.1. Dans la définition de « cluster », à l'article 1^{er}, § 1^{er}, 2^o, de l'accord de coopération, les mots « des collectivités ou des communautés » seront remplacés par les mots « des collectivités », le terme « communauté » figurant déjà dans la définition de « collectivité » à l'article 1^{er}, § 1^{er}, 3^o.

17.2. L'article 1^{er}, § 1^{er}, 6^o, de l'accord de coopération fait état d'un accord de coopération conclu entre l'INAMI et Sciensano. Les délégués ont déclaré que, ce faisant, il est fait référence à la base de données créée auprès de Sciensano en exécution d'une convention de collaboration avec l'INAMI, visée à l'article 22, 20^o, de la loi 'relative à l'assurance obligatoire soins de santé et indemnités', coordonnée le 14 juillet 1994⁴⁷. Par souci de clarté, mieux vaudrait faire référence à cette disposition législative.

Cette observation vaut également pour l'article 3, § 1^{er}, 4^o, et l'article 15, § 2, de l'accord de coopération.

18. L'article 1^{er}, § 6, alinéa 2, de l'accord de coopération prévoit que « par dérogation à l'article 458 du Code pénal, les personnes contactées sont relevées de leur obligation de garder le secret dans le cadre du présent accord de coopération ». Au regard du principe de légalité en matière pénale, il conviendrait d'indiquer plus précisément de quelles personnes il s'agit. Les délégués ont en tout cas fait savoir qu'il s'agit des personnes contactées par les centres de contact, à savoir les Personnes de catégorie II dans la mesure où le test de dépistage du COVID-19 a révélé qu'elles sont infectées, de même que les Personnes de catégorie III.

Article 3

19. L'article 3, § 2, 2^o, B, de l'accord de coopération fait mention des Personnes de catégorie V et VI, alors que son article 7, § 4, auquel il est renvoyé, mentionne uniquement les Personnes de catégorie VI. Les délégués ont reconnu qu'il s'agit d'une erreur matérielle, qui sera rectifiée.

20. Tel qu'il est formulé, l'article 3, § 3, de l'accord de coopération donne à penser que les équipes mobiles et les inspections d'hygiène compétentes ne peuvent pas traiter les données à caractère personnel des Personnes de catégorie IV. Les auteurs de l'accord de coopération vérifieront si telle est l'intention et, le cas échéant, adapteront la disposition concernée.

Article 6

21. L'article 6, §§ 2 et 4, de l'accord de coopération renvoie au numéro NISS ainsi qu'au numéro d'identification du Registre national. Le choix d'utiliser ces numéros d'identification⁴⁸ est justifié dans le commentaire général de l'accord de coopération comme suit :

« En vue de l'identification sans équivoque des personnes concernées (c'est-à-dire les patients hospitalisés, les personnes infectées ou les personnes gravement suspectées d'être infectées) et de la mise en relation des données collectées, il est absolument

⁴⁷ Ajouté par la loi 10 avril 2014 'portant des dispositions diverses en matière de santé'.

⁴⁸ Voir aussi la critique formulée dans l'avis n° 42/2020 de l'Autorité de protection des données du 25 mai 2020, observation 19.

indispensable de conserver également le numéro d'identification de sécurité sociale des personnes concernées dont les données sont traitées dans la Base de données I et de permettre un accès général au registre national. Cela soulage également les médecins, les hôpitaux et les laboratoires qui mettent les informations à disposition (c'est-à-dire les informateurs), car ils n'ont à fournir que les données qui ne se trouvent pas dans le registre national. Étant donné que l'ensemble du système de soins de santé en Belgique repose sur l'utilisation du numéro du registre national pour identifier effectivement un patient, ce numéro est également essentiel pour le traitement dans le cadre du suivi manuel des contacts, en vue d'identifier correctement la personne index ainsi que les personnes avec lesquelles la personne index a été en contact ».

Les délégués ont encore apporté la précision complémentaire suivante :

« Het verplicht gebruik van het identificatienummer van de sociale zekerheid als uniek identificatienummer in de gezondheidssector is overigens geregeld door artikel 8 van de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealthplatform. Het Grondwettelijk Hof heeft in zijn arrest 29/2010 van 18 maart 2010 geoordeeld dat 'rekening houdend met de waarborgen waarin de wet van 21 augustus 2008 voorziet met betrekking tot de vertrouwelijkheid van de persoonlijke gezondheidsgegevens gedurende de verwerking ervan door het eHealth-platform, is de keuze om gebruik te maken van het rijksregisternummer, als identificatiesleutel, in redelijkheid verantwoord' ».

Ainsi que les délégués l'ont eux-mêmes suggéré, mieux vaudrait faire figurer cette explication complémentaire dans le commentaire général précité.

22. À l'article 6, § 4, de l'accord de coopération, il y a probablement lieu d'écrire « Base de données III » au lieu de « Base de données I ».

23. L'article 6, § 5, 7°, de l'accord de coopération mentionne comme l'une des catégories de données à caractère personnel à traiter dans la Base de données I « les données nécessaires permettant au centre de contact et aux équipes mobiles de prendre tous autres contacts utiles avec la personne visée au présent paragraphe et la liste des personnes avec lesquelles la personne visée au présent paragraphe a eu des contacts, en ce compris le code postal et la langue, ainsi que le risque estimé de contagion de la personne visée au présent paragraphe ».

On n'aperçoit toutefois pas clairement le rapport entre les coordonnées des personnes concernées et le risque estimé d'infection. En outre, cette dernière donnée semble faire double emploi avec ce que mentionne l'article 6, § 5, 9°, de l'accord de coopération.

Cette observation s'applique *mutatis mutandis* également à l'article 7, § 3, 7° et 9°, de l'accord de coopération.

Article 8

24. L'article 8, 1°, de l'accord de coopération fait état du « numéro d'identification provenant d'une source authentique ». Les délégués ont déclaré que l'on vise ainsi le Registre national et la Banque-carrefour de la sécurité sociale. Mieux vaudrait le préciser.

Article 10

25. Les délégués ont confirmé que l'article 10, § 1^{er}, de l'accord de coopération fait erronément référence aux Personnes de catégorie V. Dès lors la mention de cette catégorie sera omise.

26. Les délégués ont également confirmé que la mention générale de « maladies infectieuses » à l'article 10, § 2, de l'accord de coopération est erronée et qu'il y a spécifiquement lieu de faire mention du COVID-19.

Articles 11 et 12

27. Les articles 11, § 3, et 12, § 1^{er}, 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'information⁴⁹, 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 politique⁵⁰.

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.

⁴⁹ Voir d'ailleurs à cet égard la critique qu'avait déjà formulée le Conseil d'État en la matière dans son avis C.E. 63.202/2 du 26 avril 2018 sur un avant-projet devenu 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', *Doc. parl.*, Chambre, 2017-18, n° 54-3185/001, pp. 140-142.

⁵⁰ Comparer avec les critères d'évaluation qu'utilise la Cour constitutionnelle pour apprécier les délégations de pouvoir réglementaire par le législateur à une autorité administrative autonome ou à un organisme public décentralisé; voir C.C., 11 juin 2015, n° 86/2015, B.22.4 et C.C., 9 juin 2016, n° 89/2016, B.9.6.4 : « Les articles 33, 105 et 108 de la Constitution ne s'opposent pas à ce que, dans une matière technique déterminée, le législateur confie des compétences exécutives spécifiques à une autorité administrative autonome soumise tant au contrôle juridictionnel qu'au contrôle parlementaire et n'interdisent pas au législateur d'accorder des délégations à un organe exécutif, pour autant qu'elles portent sur l'exécution de mesures dont le législateur compétent a déterminé l'objet, en particulier dans les matières techniques et complexes »; voir C.C., 9 novembre 2015, n° 162/2015, B.8.4 : « L'article 33 de la Constitution et l'article 20 de la loi spéciale du 8 août 1980 ne s'opposent pas à ce que le législateur confie des compétences exécutives spécifiques à un organisme public décentralisé qui est soumis à une tutelle administrative et à un contrôle juridictionnel ».

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.

28. Outre les observations qui précèdent, la portée de l'article 11 de l'accord de coopération gagnerait à être clarifiée.

En effet, la section de législation se demande, tout comme l'Autorité de protection des données, ce qu'il faut entendre par

« Dans la mesure où cela n'est pas repris dans le présent accord de coopération, tant la communication de données à caractère personnel à Sciensano pour traitement dans la Base de données I que la communication ultérieure de ces données à caractère personnel par Sciensano à des tiers ont toujours lieu après délibération de la Chambre « Sécurité sociale et Santé » du Comité de sécurité de l'information [...] ».

Comme le relève l'Autorité de protection des données,

« Chaque prestataire de soin (y compris donc chaque médecin) ou organisation de la santé ou de soin doit-il systématiquement soumettre chacune de ses communications à une délibération du Comité de sécurité de l'information ? Cette approche semble très lourde administrativement. Ou s'agit-il d'une délibération par catégorie de source et quelles sont alors les différentes catégories ? »⁵¹.

Par souci de sécurité juridique, la formulation de l'article 11 sera revue.

29. L'article 12, § 3, de l'accord de coopération impose une délibération de la Chambre Sécurité sociale et Santé du Comité de sécurité de l'information « dans la mesure où la communication de ces données à caractère personnel supplémentaires est nécessaire aux finalités de traitement définies à l'article 3 ».

Ainsi formulée, la disposition manque de clarté.

Si telle est l'intention, elle sera revue afin d'énoncer que l'autorisation ne peut être accordée qu'à la condition que la communication des données à caractère personnel supplémentaires soit nécessaire aux finalités de traitement définies à l'article 3.

Article 14

30. Dans un souci de sécurité juridique, la terminologie utilisée à l'article 14 de l'accord de coopération pour désigner « l'application numérique de traçage des contacts » sera uniformisée.

Par ailleurs, la « Base de données V » étant définie à l'article 1^{er}, 9^o, comme étant

⁵¹ Avis n° 36/2020, point 36.

« le journal central des enregistrements [...] », il n'est pas nécessaire, à l'article 14, de faire référence au « journal central des enregistrements de la Base de données V »⁵². L'on se contentera de se référer à la Base de données V.

31. L'article 14 ne précise pas qui aura accès à la Base de données V. S'il s'agit seulement du responsable du traitement, à savoir Sciensano, il convient de le préciser expressément.

Par ailleurs, ainsi que le relève l'Autorité de protection des données, « il convient de préciser clairement quels sont les traitements de données réalisés par Sciensano pour assurer le fonctionnement du système de traçage »⁵³.

32. L'article 14, § 2, 2°, prévoit le signalement d'une infection au COVID-19 par un utilisateur « de manière anonymisée, ou au moins pseudonymisée ».

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.

Interrogé quant à la nécessité de prévoir une possibilité de pseudonymisation, les délégués ont répondu ce qui suit :

« Technisch gezien zou men kunnen stellen dat de beveiligde sleutels die gebruikt worden op het toestel van de gebruiker en eigen zijn aan een gebruiker, alsnog (en enkel door gebruik te maken van hacking-technieken) zouden kunnen toelaten om de gedeelde serienummers van diezelfde gebruiker te ontsleutelen en terug te koppelen aan die gebruiker. Dus hoewel eerder theoretisch van aard, bestaat er dus nog een sleutel, vandaar dat de gegevens eerder als gepseudonimiseerd moeten beschouwd worden, dan geanonimiseerd. De toegang tot deze beveiligde sleutels is afgeschermd, ook voor de gebruiker. Enkel met toegang tot het toestel en de nodige hackingtechnieken zou men eventueel in staat kunnen zijn om de sleutel te achterhalen. Het enige wat daar dan nog uit zou kunnen geleerd worden, is of de gebruiker zich gemeld heeft als besmette gebruiker of niet. Centraal kan er echter niets ontsleuteld worden. Ook andere gebruikers kunnen op geen enkele manier de gedeelde serienummers terugkoppelen aan een individu ».

À la lumière de cette réponse, le dispositif à l'examen paraît admissible.

33. À l'article 14, § 3, 2°, il conviendrait de préciser ce que l'on entend par une application mobile installée « localement ».

Au 14° du même paragraphe, par souci de sécurité juridique, il conviendrait, au moins dans le commentaire général, de préciser ce que l'on entend par le « code source complet » et la « couche application ». La formulation de cette disposition sera par ailleurs revue.

34. L'article 14, § 5, alinéa 1^{er}, dispose que l'installation, l'utilisation et la

⁵² Voir notamment l'article 14, § 3, 3°, 9° et 10°.

⁵³ Avis n° 43/2020, point 25.

désinstallation de l'application numérique de traçage des contacts par un utilisateur se font exclusivement de manière volontaire.

À cet égard, la section de législation a déjà fait observer ce qui suit :

« La question se pose toutefois de savoir si cette disposition, dans sa formulation générale, tient compte suffisamment de l'article 8 du RGPD, qui fixe des conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information et qui prescrit que pour les enfants âgés de moins de 16 ans (ou qui éventuellement ne sont pas âgés de moins de 13 ans)⁵⁴, le consentement doit être donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. Compte tenu des moyens technologiques disponibles, le responsable du traitement doit raisonnablement s'efforcer de vérifier que ce consentement requis est donné (ou autorisé). Bien que la disposition réglementaire précitée soit directement applicable et qu'elle soit dès lors contraignante pour le responsable du traitement, il peut néanmoins être envisagé de compléter la proposition de loi par des dispositions qui concrétisent cette obligation pour l'application concernée »⁵⁵.

Pareille observation peut être réitérée.

35. L'article 14, § 5, alinéa 2, dispose que « l'installation ou non, l'utilisation ou non et la désinstallation ou non de l'application mobile de l'application numérique de traçage des contacts ne peuvent donner lieu à [...] aucun avantage ou désavantage ».

À cet égard, la section de législation a déjà fait observer ce qui suit :

« Il est probablement impossible de définir de manière concluante les termes « quelconque avantage ou désavantage » dans le texte de la proposition même, mais il n'en demeure pas moins que sur la base du texte actuel et de ses développements, on n'aperçoit pas clairement si, par exemple, l'application peut être liée à d'autres applications intéressantes pour l'utilisateur ou si certaines réductions peuvent être associées à l'utilisation de l'application, etc. Il est dès lors conseillé de développer quelque peu la casuistique dans le cadre des débats parlementaires »⁵⁶.

Interrogés à cet égard, les délégués ont apporté les précisions suivantes :

« Een werkgever mag bijvoorbeeld zijn werknemers niet verplichten om de contactsporingsapplicatie te installeren. Dit mag op geen enkele wijze geschieden, en aldus ook niet door daar bepaalde voor- of nadelen te koppelen aan het al dan niet installeren van de contactsporingsapplicatie. Zo zal het bijvoorbeeld niet toegelaten zijn om een werknemer een bonus te geven voor het installeren van de contactsporingsapplicatie, of een deel van het loon in te houden ten gevolge van het niet installeren van de app, of werknemers de toegang tot de gebouwen te ontzeggen bij niet gebruik van de contactsporingsapplicatie. Leveranciers van goederen en diensten mogen het gebruik of niet gebruik van de contactsporingsapplicatie niet linken aan hun goederen of diensten of een voorwaarde maken voor het verkrijgen van hun goederen en diensten. Bijvoorbeeld kortingen aanbieden bij gebruik van de app, toegang weigeren bij

⁵⁴ Note de bas de page n° 29 de l'avis cité : Si l'on choisit d'appliquer un âge inférieur à 16 ans, conformément à l'article 8, paragraphe 1, deuxième alinéa, du RGPD.

⁵⁵ Avis n° 67.424/3.

⁵⁶ *Ibidem*.

niet gebruik van de app (bioscoop, luchthaven, winkel, openbaar vervoer, taxi, vliegtuig, horeca, enz.).

Indien gewenst kan dit verder worden toegelicht in de algemene toelichting van het samenwerkingsakkoord ».

De telles précisions permettent effectivement d'appréhender plus clairement la portée de l'expression « aucun avantage ou désavantage ». Elles seront reprises dans le commentaire général.

36. Il est renvoyé à l'observation particulière relative à l'article 15 en ce qui concerne la motivation du choix de la durée de trois semaines.

37. L'article 14, § 2 ne prévoit pas expressément, parmi les finalités poursuivies par le traitement des données à caractère personnel, le traitement complémentaire de données à caractère personnel en vue de la recherche scientifique et épidémiologique. Aucune finalité de recherche épidémiologique ne semble donc poursuivie par l'application numérique de traçage des contacts⁵⁷.

L'article 14, § 7, alinéa 2, prévoit toutefois la possibilité de traiter les informations collectées

« conformément aux conditions prévues au titre 4 de la loi du 30 juillet 2018 à l'égard des traitements de données à caractère personnel à des fins archivistiques d'intérêt général, à des fins de recherche scientifique ou historique ou à des fins statistiques visées à l'article 89, §§ 2 et 3 du RGPD ».

Interrogés à cet égard, les délégués ont répondu ce qui suit :

« Enkel het loutere antwoord op de vraag of men al dan niet gebruik maakt van een applicatie zal worden meegenomen in de gegevensuitwisseling naar Gegevensbank II. Het bewaren van bijkomende gegevens, louter met het oog op wetenschappelijk onderzoek en ingeval van een opt-in door de gebruiker, werd bij de uitwerking van dit akkoord niet langer opportuun geacht, onder meer omwille van de bezorgdheid om een duidelijke communicatie ten aanzien van de burger te kunnen voeren met betrekking tot de doelstellingen van de applicatie ».

Si telle est l'intention, l'article 14, § 7, alinéa 2, sera omis.

38. Il convient de compléter l'article 14 afin de préciser qui est chargé de décider quelle(s) application(s) seront mises à disposition du public, après vérification de leur conformité aux règles édictées dans l'accord de coopération⁵⁸ et qui sera par la suite chargé de leur désactivation à l'échéance de la période de validité d'utilisation de celle(s)-ci⁵⁹.

⁵⁷ Ainsi que l'avait recommandé l'Autorité de protection des données (voir l'avis n° 43/2020, point 30).

⁵⁸ Voir dans le même sens l'avis de l'Autorité de protection des données n° 43/2020, point 21.

⁵⁹ *Ibidem*, point 35.

Article 15

39.1. À l'instar de ce qui figure dans le commentaire général de l'accord de coopération s'agissant du délai de soixante jours retenu pour les données de la Base de données centrale, il conviendrait de justifier le choix des délais de conservation des données à caractère personnel retenus pour les autres Bases de données.

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

« Na een termijn van 10 jaar worden de gegevens ofwel gewist, ofwel nagekeken op hun accurateheid en indien nodig geüpdatet. Indien in geval van niet-accurate gegevens updaten onmogelijk is of niet opportuun, zullen de gegevens gewist worden. Zolang ze niet gewist zijn, zijn ze accuraat en zijn dit de gegevens van de contactpersonen van de collectiviteiten. In geval van uitbraken van andere infectieziekten, zal dit immers zeer nuttig zijn ».

Cette absence de délai maximal de conservation pour ces données à caractère personnel n'est toutefois pas conforme à l'article 5, paragraphe 1, e), du RGDP, qui prescrit que

« les données à caractère personnel doivent être [...] conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées »⁶⁰.

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

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

Le dispositif sera revu de manière à rendre celui-ci conforme au principe selon lequel il appartient au législateur de fixer les délais de conservation des données à caractère personnel.

39.3. Aucune justification n'a été fournie par les délégués concernant l'exception prévue pour la Base de données V. À défaut de justification, il convient par conséquent de prévoir une disposition équivalente au paragraphe 1^{er}, alinéa 2, pour la suppression des données à caractère personnel de la Base de données V.

40. Au paragraphe 2, il convient de préciser les dispositions de la loi du 10 avril 2014 'portant des dispositions diverses en matière de santé' auxquelles il est fait référence.

⁶⁰ Voir également l'avis n^{os} 37.748 et 37.749/AG donné le 23 novembre 2004 sur un avant-projet devenu la loi du 3 mai 2005 'modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité' (37.748/AG) et sur un avant-projet devenu la loi du 3 mai 2005 'modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité' (37.749/AG), *Doc. parl.*, Chambre, 2004-2005, n^{os} 51-1598/1 et 51-1599/1, pp. 45 à 77, <http://www.raadvst-consetat.be/dbx/avis/37748.pdf>.

Interrogés à cet égard, les délégués ont répondu ce qui suit :

« Hiermee wordt naar artikel 16 van de wet van 10 april 2014 verwezen ».

Le paragraphe 2 sera par conséquent complété en ce sens.

Article 16

41. Interrogés quant à la portée de l'article 16, § 4, de l'accord de coopération, les délégués ont répondu ce qui suit :

« Hier wordt een overeenkomst bedoeld die enerzijds elementen heeft van de overeenkomst die normaal wordt afgesloten tussen de verwerkingsverantwoordelijke en de verwerker, en anderzijds een overeenkomst die normaal wordt afgesloten tussen verschillende verwerkingsverantwoordelijken voor de overdracht van persoonsgegevens.

Het uitgangspunt van een dergelijke overeenkomst tussen Sciensano en de deelstaten is dat er een gemeenschappelijk beleid is inzake het tegemoetkomen aan de rechten van de betrokkenen. Immers, onder de AVG heeft elke verwerkingsverantwoordelijke de plicht om te reageren op verzoeken van de betrokkene omtrent zijn of haar rechten. Hierbij kan gedacht worden aan bijvoorbeeld het recht op inzage. Echter, omwille van het feit dat het voor de betrokkene weinig opportuun is om zijn of haar verzoek te richten aan elke verwerkingsverantwoordelijke afzonderlijk, moeten hiervoor afspraken worden gemaakt tussen de verwerkingsverantwoordelijken onderling. In de overeenkomst kan bijvoorbeeld worden bepaald dat één partij optreedt als een single point of contact die alle verzoeken van de betrokkenen behandelt ».

Les responsabilités respectives de Sciensano, des autorités et agences compétentes concernées en ce qui concerne l'exercice des droits de la personne concernée et la fourniture d'information ne peuvent pas être fixées par le biais d'un règlement conclu entre Sciensano, les entités fédérées et les agences. Un tel instrument peut certes être utile pour harmoniser et coordonner la politique, mais les accords qu'il contient doivent être traduits dans des règles de droit formelles, d'autant plus qu'il s'agit précisément de l'exercice des droits des particuliers et de leur information.

Article 17

42.1. Il convient de mentionner l'intitulé complet de la loi spéciale du 8 aout 1980 'de réformes institutionnelles'.

42.2. Comme en ont convenu les délégués, conformément à l'article 92bis, § 5, alinéas 4 et 8, de la loi spéciale du 8 aout 1980, l'accord de coopération sera complété par le règlement du mode de désignation des membres de la juridiction autres que le président et par le règlement des frais de fonctionnement de la juridiction ⁶¹.

⁶¹ Voir Y. PEETERS, *De plaats van samenwerkingsakkoorden in het constitutioneel kader*, Bruges, die Keure, 2016, pp. 329-330.

Article 19

43. Conformément à l'article 19, § 1^{er}, de l'accord de coopération, celui-ci entre en vigueur (lire : produit ses effets) le 4 mai 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 ⁶².

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 67.425/3-67.427/3 et 67.424/3, un effet rétroactif peut, dans ces circonstances, être conféré aux dispositions de l'accord de coopération, qui correspondent sur le fond à la réglementation portée par l'arrêté royal n° 18 du 4 mai 2020, avec effet à la date d'entrée en vigueur de cet arrêté, soit le 4 mai 2020.

Cette justification ne vaut cependant pas pour les nouveaux éléments qui ont été ajoutés à l'accord de coopération par rapport à l'arrêté royal n° 18 du 4 mai 2020. Pour ce motif, il serait préférable de compléter l'article 19, § 1^{er}, de l'accord de coopération comme suit : « , en ce qui concerne les dispositions qui correspondent sur le fond à l'arrêté royal n° 18 du 4 mai 2020 portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19, tel qu'il était applicable à partir du 4 mai 2020 ».

Cette justification ne s'applique pas non plus à l'article 14 de l'accord de coopération, qui porte sur les applications numériques de traçage de contacts, dès lors que de telles applications n'ont pas encore été mises en service et qu'un effet rétroactif à cette fin est donc inutile. Il convient par conséquent d'exclure cet article de la rétroactivité.

EXAMEN DE L'AVANT-PROJET DE LOI

44. Il convient de compléter l'intitulé de l'avant-projet et l'article portant assentiment à l'accord de coopération par la date à laquelle l'accord de coopération a été signé.

45. L'article 6 de l'avant-projet comporte une disposition d'entrée en vigueur. Pareille disposition dans un texte d'assentiment n'a guère de sens et peut même être source d'insécurité juridique, dès lors que les effets dans le temps de l'accord de coopération sont réglés à l'article 19, § 1^{er}, de l'accord de coopération proprement dit et que celui-ci ne peut pas entrer en

⁶² Jurisprudence constante de la Cour constitutionnelle, voir notamment : C.C., 21 novembre 2013, n° 158/2013, B.24.2; C.C., 19 décembre 2013, n° 172/2013, B.22; C.C., 29 janvier 2014, n° 18/2014, B.10; C.C., 9 octobre 2014, n° 146/2014, B.10.1; C.C., 22 janvier 2015, n° 1/2015, B.4; C.C., 7 mai 2015, n° 54/2015, B.12; C.C., 14 janvier 2016, n° 3/2016, B.22; C.C., 3 février 2016, n° 16/2016, B.12.1; C.C., 28 avril 2016, n° 58/2016, B.9.2; C.C., 9 février 2017, n° 15/2017, B.9.2.

vigueur avant le jour de la publication de l'acte d'assentiment publié en dernier lieu ⁶³. Par conséquent, il y a lieu d'omettre l'article 6.

DE GRIFFIER - LE GREFFIER

DE VOORZITTER - LE PRÉSIDENT

Annemie GOOSSENS

Jo BAERT

⁶³ Y. PEETERS, *De plaats van samenwerkingsakkoorden in het constitutioneel kader*, o.c., pp. 268-269.