UITVOERINGSBESLUIT (EU) 2022/483 VAN DE COMMISSIE

van 21 maart 2022

tot wijziging van Uitvoeringsbesluit (EU) 2021/1073 tot vaststelling van technische specificaties en regels voor de uitvoering van het bij Verordening (EU) 2021/953 van het Europees Parlement en de Raad vastgestelde vertrouwenskader voor het digitaal EU-covidcertificaat

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2021/953 van het Europees Parlement en de Raad van 14 juni 2021 betreffende een kader voor de afgifte, verificatie en aanvaarding van interoperabele COVID-19-vaccinatie-, test- en herstelcertificaten (digitaal EU-covidcertificaat) teneinde het vrije verkeer tijdens de COVID-19-pandemie te faciliteren ([1]), en met name artikel 9, lid 1,

Overwegende hetgeen volgt:

(1) Bij Verordening (EU) 2021/953 is het digitaal EU-covidcertificaat vastgesteld, dat bewijst dat een persoon gevaccineerd is tegen COVID-19, negatief is getest of van COVID-19 is hersteld, teneinde de uitoefening van het recht op vrij verkeer door de houders tijdens de COVID-19-pandemie te vergemakkelijken.

(2) Verordening (EU) 2021/954 van het Europees Parlement en de Raad ([2]) bepaalt dat de lidstaten de regels van Verordening (EU) 2021/953 toepassen op onderdanen van derde landen die niet binnen het toepassingsgebied van die verordening vallen, maar die legaal op hun grondgebied verblijven of wonen en overeenkomstig het Unierecht het recht hebben naar andere lidstaten te reizen.

(3) In Aanbeveling (EU) 2022/290 van de Raad tot wijziging van Aanbeveling (EU) 2020/912 over de tijdelijke beperking van niet-essentiële reizen naar de EU en de mogelijke opheffing van die beperking ([3]) is bepaald dat onderdanen van derde landen die niet-essentiële reizen vanuit een derde land naar de Unie wensen te ondernemen, in het bezit moeten zijn van een geldig bewijs van vaccinatie of herstel, zoals een digitaal EU-covidcertificaat of een COVID-19-certificaat afgegeven door een derde land dat onder een krachtens artikel 8, lid 2, van Verordening (EU) 2021/953 vastgestelde uitvoeringshandeling valt.

(4) Om ervoor te zorgen dat het digitale EU-covidcertificaat in de hele Unie kan worden gebruikt, heeft de Commissie Uitvoeringsbesluit (EU) 2021/1073 ([4]) vastgesteld waarin technische specificaties en regels zijn opgenomen voor het invullen, beveiligd afgeven en verifiëren van de digitale EU-covidcertificaten, de beveiliging van de persoonsgegevens, het vaststellen van de gemeenschappelijke structuur van de unieke certificaatidentificatiecode en de afgifte van een geldige, beveiligde en interoperabele barcode.

(5) Overeenkomstig artikel 4 van Verordening (EU) 2021/953 moesten de Commissie en de lidstaten een vertrouwenskader voor het digitaal EU-covidcertificaat opzetten en in stand houden. Dat vertrouwenskader kan steun verlenen aan de bilaterale uitwisseling van lijsten van ingetrokken certificaten met de unieke certificaatidentificatiecodes van ingetrokken certificaten.

([1]) PB L 211 van 15.6.2021, blz. 1.

([2]) Verordening (EU) 2021/954 van het Europees Parlement en de Raad van 14 juni 2021 betreffende een kader voor de afgifte, verificatie en aanvaarding van interoperabele COVID-19-vaccinatie-, test- en herstelcertificaten (digitaal EU-covidcertificaat) ten aanzien van onderdanen van derde landen die legaal op het grondgebied van de lidstaten verblijven of wonen tijdens de COVID-19-pandemie (PB L 211 van 15.6.2021, blz. 24).

([3]) Aanbeveling (EU) 2022/290 van de Raad van 22 februari 2022 tot wijziging van Aanbeveling (EU) 2020/912 over de tijdelijke beperking van niet-essentiële reizen naar de EU en de mogelijke opheffing van die beperking (PB L 43 van 24.2.2022, blz. 79)

([4]) Uitvoeringsbesluit (EU) 2021/1073 van de Commissie van 28 juni 2021 tot vaststelling van technische specificaties en regels voor de uitvoering van het bij Verordening (EU) 2021/953 van het Europees Parlement en de Raad vastgestelde vertrouwenskader voor het digitaal EU-covidcertificaat (PB L 230 van 30.6.2021, blz. 32).

(6) De gateway voor digitale EU-covidcertificaten (de "gateway"), die het centrale onderdeel is van het vertrouwenskader en die de veilige en betrouwbare uitwisseling tussen de lidstaten van openbare sleutels voor de verificatie van digitale EU-covidcertificaten mogelijk maakt, is op 1 juli 2021 operationeel geworden.

(7) Dankzij de succesvolle en grootschalige uitrol ervan zijn digitale EU-covidcertificaten een doelwit geworden voor fraudeurs die zoeken naar manieren om frauduleuze certificaten af te geven. Die frauduleuze certificaten moeten daarom worden ingetrokken. Daarnaast kunnen bepaalde digitale EU-covidcertificaten door de lidstaten op nationaal niveau worden ingetrokken om medische en volksgezondheidsredenen, bijvoorbeeld omdat een partij toegediende vaccins later ondeugdelijk is gebleken.

(8) Hoewel het systeem van digitale EU-covidcertificaten vervalste certificaten onmiddellijk kan opsporen, kunnen op basis van valse documenten, ongeoorloofde toegang of met frauduleuze bedoelingen onrechtmatig afgegeven authentieke certificaten in andere lidstaten niet worden ontdekt, tenzij op nationaal niveau gegenereerde lijsten van ingetrokken certificaten tussen de lidstaten worden uitgewisseld. Hetzelfde geldt voor certificaten die om medische en volksgezondheidsredenen zijn ingetrokken. Wanneer de certificaten die door lidstaten zijn ingetrokken niet door de verificatietoepassingen van de andere lidstaten kunnen worden opgespoord, komt de volksgezondheid in gevaar en wordt het vertrouwen van de burgers in het systeem van digitale EU-covidcertificaten ondermijnd.

(9) Zoals in overweging 19 van Verordening (EU) 2021/953 wordt aangegeven, moeten de lidstaten, om medische en volksgezondheidsredenen en in geval van op frauduleuze wijze afgegeven of verkregen certificaten voor de toepassing van deze verordening in beperkte gevallen lijsten van ingetrokken certificaten kunnen opstellen en die uitwisselen met andere lidstaten, met name om certificaten in te trekken die ten onrechte of als gevolg van fraude zijn afgegeven, of na het stopzetten van vaccinatie met een partij COVID-19-vaccins die ondeugdelijk is gebleken. De lidstaten mogen door andere lidstaten afgegeven certificaten niet kunnen intrekken. De uitgewisselde lijsten van ingetrokken certificaten mogen behalve de unieke certificaatidentificatiecodes geen persoonsgegevens bevatten. Met name mogen zij niet vermelden waarom een certificaat is ingetrokken.

(10) Naast de algemene informatie over de mogelijke intrekking van certificaten en de mogelijke redenen daarvoor, moeten houders van ingetrokken certificaten onverwijld door de verantwoordelijke autoriteit van afgifte in kennis worden gesteld van de intrekking van hun certificaten en de redenen voor de intrekking. In sommige gevallen, en met name in het geval van digitale EU-covidcertificaten die op papier worden afgegeven, kan het echter onmogelijk blijken of een onevenredige inspanning vergen om de houder op te sporen en van de intrekking in kennis te stellen. De lidstaten mogen geen aanvullende persoonsgegevens verzamelen die niet nodig zijn voor het afgifteproces, alleen om certificaathouders te kunnen informeren wanneer hun certificaten worden ingetrokken.

(11) Daarom moet het vertrouwenskader voor digitale EU-covidcertificaten worden versterkt door de bilaterale uitwisseling van lijsten van ingetrokken certificaten tussen de lidstaten te ondersteunen.

(12) Dit besluit heeft geen betrekking op de tijdelijke schorsing van certificaten voor gevallen van nationaal gebruik die buiten het toepassingsgebied van de verordening inzake het digitaal EU-covidcertificaat vallen, bijvoorbeeld omdat de houder van een vaccinatiecertificaat positief heeft getest op SARS-CoV-2. Dit besluit doet geen afbreuk aan vastgestelde procedures voor de controle van de bedrijfsregels voor de geldigheid van certificaten.

(13) Hoewel uit technisch oogpunt verschillende architecturen voor de uitwisseling van intrekkingslijsten haalbaar zijn, is de uitwisseling ervan via de gateway het meest geschikt, aangezien dit de uitwisseling van gegevens beperkt tot het reeds vastgestelde vertrouwenskader en het zowel het aantal zwakken punten als het aantal uitwisselingen tussen de lidstaten tot een minimum beperkt in vergelijking met een alternatief peer-to-peersysteem.

(14) De gateway voor digitale EU-covidcertificaten moet dan ook worden versterkt om de veilige uitwisseling van ingetrokken digitale EU-covidcertificaten te ondersteunen met het oog op de veilige verificatie ervan via de gateway. In dit verband moeten passende beveiligingsmaatregelen worden genomen ter bescherming van de persoonsgegevens die in de gateway worden verwerkt. Om een hoog beschermingsniveau te waarborgen, moeten de lidstaten de attributen van certificaten pseudonimiseren door middel van een onomkeerbare hash die in de intrekkingslijsten moet worden opgenomen. De unieke identificatiecode moet worden beschouwd als gepseudonimiseerde data voor de verwerkingshandelingen binnen het kader van de gateway.

(15) Voorts moeten bepalingen worden vastgesteld over de rol van de lidstaten en de Commissie bij de uitwisseling van lijsten van ingetrokken certificaten.

(16) De verwerking van persoonsgegevens van certificaathouders, die plaatsvindt onder de verantwoordelijkheid van de lidstaten of andere overheidsorganisaties of officiële instanties in de lidstaten, moet worden uitgevoerd in overeenstemming met Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([5]). De verwerking van persoonsgegevens onder de verantwoordelijkheid van de Commissie met het oog op het beheer en de waarborging van de beveiliging van de gateway voor digitale EU-covidcertificaten moet geschieden conform Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([6]).

(17) De lidstaten, vertegenwoordigd door de aangewezen nationale autoriteiten of officiële instanties, bepalen gezamenlijk de doeleinden van en de middelen voor de verwerking van persoonsgegevens via de gateway voor digitale EU-covidcertificaten en zijn derhalve gezamenlijke verwerkingsverantwoordelijken. Op grond van artikel 26 van Verordening (EU) 2016/679 zijn gezamenlijke verwerkingsverantwoordelijken op het gebied van de verwerking van persoonsgegevens verplicht om op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van die verordening vast te stellen. Dat artikel voorziet ook in de mogelijkheid om die verantwoordelijkheden te laten vaststellen bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de gezamenlijke verwerkingsverantwoordelijken van toepassing is. De in artikel 26 bedoelde regelingen moeten worden opgenomen in bijlage III bij dit besluit.

(18) Bij Verordening (EU) 2021/953 is de Commissie belast met de ondersteuning van dergelijke uitwisselingen. De meest geschikte manier om dat mandaat te vervullen is het verzamelen van de namens de lidstaten ingediende lijsten van ingetrokken certificaten. Daarom moet de Commissie een rol van gegevensverwerker krijgen om deze uitwisselingen te ondersteunen door de uitwisseling van lijsten via de gateway voor digitale EU-covidcertificaten namens de lidstaten te vergemakkelijken.

(19) Als aanbieder van technische en organisatorische oplossingen voor de gateway voor digitale EU-covidcertificaten verwerkt de Commissie de persoonsgegevens in de intrekkingslijsten in de gateway namens de lidstaten als gezamenlijke verwerkingsverantwoordelijken. Daarom treedt zij op als verwerker. Krachtens artikel 28 van Verordening (EU) 2016/679 en artikel 29 van Verordening (EU) 2018/1725 moet de verwerking door een verwerker worden geregeld in een overeenkomst of een rechtshandeling naar het recht van de Unie of van de lidstaten die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt en de verwerking specificeert. Daarom moeten regels worden vastgesteld voor de verwerking door de Commissie als gegevensverwerker.

(20) De ondersteunende taken van de Commissie omvatten niet de oprichting van een gecentraliseerde databank als bedoeld in overweging 52 van Verordening (EU) 2021/953. Dat verbod is bedoeld om een centraal register van alle afgegeven digitale EU-covidcertificaten te voorkomen en belet de lidstaten niet om intrekkingslijsten uit te wisselen, zoals uitdrukkelijk is bepaald in artikel 4, lid 2, van Verordening (EU) 2021/953.

(21) Bij de verwerking van persoonsgegevens in de gateway voor het digitale EU-covidcertificaat is de Commissie gebonden door Besluit (EU, Euratom) 2017/46 van de Commissie ([7]).

(22) Op grond van artikel 3, lid 10, van Verordening (EU) 2021/953 kan de Commissie uitvoeringshandelingen vaststellen waarbij wordt vastgesteld dat COVID-19-certificaten die zijn afgegeven door een derde land waarmee de Unie en de lidstaten een overeenkomst inzake het vrije verkeer van personen hebben gesloten die de overeenkomstsluitende partijen de gelegenheid biedt het vrije verkeer omwille van de volksgezondheid op niet-discriminerende wijze te beperken en die geen mechanisme voor de opneming van rechtshandelingen van de Unie bevat, gelijkwaardig zijn aan die welke overeenkomstig deze verordening zijn afgegeven. Op basis daarvan heeft de Commissie op 8 juli 2021 Uitvoeringsbesluit (EU) 2021/1126 ([8]) tot vaststelling van de gelijkwaardigheid van de door Zwitserland afgegeven COVID-19-certificaten vastgesteld.

([5]) 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) (PB L 119 van 4.5.2016, blz. 1).

([6]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39).

([7]) De Commissie publiceert nadere informatie over de beveiligingsnormen voor alle informatiesystemen van de Europese Commissie op https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en

([8]) Uitvoeringsbesluit (EU) 2021/1126 van de Commissie van 8 juli 2021 houdende vaststelling van de gelijkwaardigheid van de door Zwitserland afgegeven COVID-19-certificaten aan de overeenkomstig Verordening (EU) 2021/953 van het Europees Parlement en de Raad afgegeven certificaten (PB L 243 van 9.7.2021, blz. 49).

(23) Op grond van artikel 8, lid 2, van Verordening (EU) 2021/953 kan de Commissie uitvoeringshandelingen vaststellen waarin wordt vastgesteld dat COVID-19-certificaten die de in de bijlage bij de verordening bedoelde gegevens bevatten en die door een derde land zijn afgegeven overeenkomstig normen en technologische systemen die interoperabel zijn met het vertrouwenskader voor het digitaal EU-covidcertificaat en die het mogelijk maken de echtheid, geldigheid en integriteit van het certificaat te verifiëren, moeten worden beschouwd als gelijkwaardig aan digitale EU-covidcertificaten, teneinde de uitoefening van het recht van vrij verkeer binnen de Unie door de houders ervan te faciliteren. Zoals opgemerkt in overweging 28 van Verordening (EU) 2021/953 heeft artikel 8, lid 2, van die verordening betrekking op de aanvaarding van door derde landen aan burgers van de Unie en hun familieleden afgegeven certificaten. De Commissie heeft reeds een aantal zodanige uitvoeringshandelingen vastgesteld.

(24) Ter voorkoming van lacunes in de opsporing van ingetrokken certificaten die onder dergelijke uitvoeringshandelingen vallen, moet het voor derde landen waarvan de COVID-19-certificaten op grond van artikel 3, lid 10, en artikel 8, lid 2, van Verordening (EU) 2021/953 gelijkwaardig worden geacht, ook mogelijk zijn om bij de gateway voor digitale EU-covidcertificaten relevante lijsten van ingetrokken certificaten in te dienen.

(25) Sommige onderdanen van derde landen die houder zijn van ingetrokken COVID-19-certificaten die door derde landen werden afgegeven en op grond van Verordening (EU) 2021/953 gelijkwaardig worden geacht, kunnen buiten het toepassingsgebied vallen van die verordening of van Verordening (EU) 2021/954 wanneer door het betrokken derde land een intrekkingslijst wordt gegenereerd waarin hun certificaten zijn opgenomen. Wanneer een betrokken derde land een lijsten van ingetrokken certificaten genereert, is evenwel niet bekend of alle onderdanen van derde landen die houder zijn van ingetrokken certificaten binnen het toepassingsgebied van een van beide verordeningen vallen. Het is dus niet haalbaar om personen die op het tijdstip waarop de lijsten worden gegenereerd niet onder het toepassingsgebied van een van deze verordeningen vallen, uit te sluiten van de lijsten van ingetrokken certificaten van die landen, en een poging daartoe zou ertoe leiden dat de lidstaten de ingetrokken certificaten van onderdanen van derde landen die voor het eerst naar de Unie reizen, niet kunnen herkennen. Maar zelfs de ingetrokken certificaten van die onderdanen van derde landen zouden worden geverifieerd door de lidstaten wanneer de houders ervan naar de Unie reizen, en als zij vervolgens binnen de Unie reizen. De derde landen waarvan de certificaten niet overeenkomstig Verordening (EU) 2021/953 als gelijkwaardig worden beschouwd, zijn niet betrokken bij het beheer van de gateway en kunnen dus niet als gezamenlijke verwerkingsverantwoordelijken worden aangemerkt.

(26) Bovendien blijkt het systeem van het digitaal EU-covidcertificaat het enige COVID-19-certificaatsysteem te zijn dat internationaal op grote schaal wordt gebruikt. Daardoor is het digitaal EU-covidcertificaat wereldwijd steeds belangrijker geworden en heeft het bijgedragen aan de aanpak van de pandemie op internationaal niveau, door veilig internationaal reizen en het wereldwijde herstel te vergemakkelijken. Bij de vaststelling van nieuwe uitvoeringshandelingen krachtens artikel 8, lid 2, van Verordening (EU) 2021/953 ontstaan nieuwe behoeften met betrekking tot het invullen van het digitaal EU-covidcertificaat. Volgens de regels van Uitvoeringsbesluit (EU) 2021/1073 is de achternaam een verplicht veld in de technische inhoud van het certificaat. Dat vereiste moet worden gewijzigd om inclusie en interoperabiliteit met andere systemen te bevorderen, aangezien er in sommige derde landen personen zijn zonder achternaam. Wanneer de naam van de certificaathouder niet in twee delen kan worden opgesplitst, moet de naam in hetzelfde veld (naam of voornaam) van het digitaal EU-covidcertificaat worden vermeld als in het reis- of identiteitsdocument van de houder. Deze wijziging zou ook de technische inhoud van de certificaten beter afstemmen op de momenteel geldige specificaties inzake machineleesbare reisdocumenten die door de Internationale Burgerluchtvaartorganisatie zijn gepubliceerd.

(27) Uitvoeringsbesluit (EU) 2021/1073 moet daarom dienovereenkomstig worden gewijzigd.

(28) Overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 is de Europese Toezichthouder voor gegevensbescherming geraadpleegd, en op 11 maart 2022 heeft hij een advies uitgebracht.

(29) Om de lidstaten en de Commissie voldoende tijd te geven om de wijzigingen door te voeren die nodig zijn om de uitwisseling van lijsten van ingetrokken certificaten via de gateway voor digitale EU-covidcertificaten mogelijk te maken, moet dit besluit vier weken na zijn inwerkingtreding van toepassing worden.

(30) De maatregelen waarin dit besluit voorziet, zijn in overeenstemming met het advies van het bij artikel 14 van Verordening (EU) 2021/953 opgerichte comité,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Uitvoeringsbesluit (EU) 2021/1073 wordt als volgt gewijzigd:

1) De volgende artikelen 5 bis, 5 ter en 5 quater worden ingevoegd:

"*Artikel 5 bis*

Uitwisseling van lijsten van ingetrokken certificaten

1. Het vertrouwenskader voor digitale EU-covidcertificaten maakt de uitwisseling van lijsten van ingetrokken certificaten mogelijk via de centrale gateway voor digitale EU-covidcertificaten (de "gateway") overeenkomstig de technische specificaties in bijlage I.

2. Lidstaten die digitale EU-covidcertificaten intrekken, kunnen lijsten van ingetrokken certificaten indienen bij de gateway.

3. Wanneer lidstaten lijsten van ingetrokken certificaten indienen, houden de autoriteiten van afgifte een lijst van ingetrokken certificaten bij.

4. Wanneer via de gateway persoonsgegevens worden uitgewisseld, blijft de verwerking beperkt tot de ondersteuning van de uitwisseling van informatie over de intrekking. Dergelijke persoonsgegevens mogen alleen worden gebruikt ter verificatie van de intrekkingsstatus van digitale EU-covidcertificaten die zijn afgegeven binnen het toepassingsgebied van Verordening (EU) 2021/953.

5. De bij de gateway ingediende informatie omvat de volgende gegevens overeenkomstig de technische specificaties in bijlage I:

a) de gepseudonimiseerde unieke certificaatidentificatiecodes van ingetrokken certificaten,

b) een vervaldatum van de ingediende lijst van ingetrokken certificaten.

6. Wanneer een autoriteit van afgifte haar op grond van Verordening (EU) 2021/953 of Verordening (EU) 2021/954 afgegeven digitale EU-covidcertificaten intrekt, en voornemens is relevante informatie uit te wisselen via de gateway, kan zij de in lid 5 bedoelde informatie in een beveiligd formaat in de vorm van lijsten van ingetrokken certificaten aan de gateway doorgeven overeenkomstig de technische specificaties in bijlage I.

7. De autoriteiten van afgifte bieden, voor zover mogelijk, een oplossing om de houders van ingetrokken certificaten op de hoogte te brengen van de intrekkingsstatus van hun certificaten en de reden voor de intrekking op het tijdstip van de intrekking.

8. De gateway verzamelt de ontvangen lijsten van ingetrokken certificaten en voorziet in instrumenten voor de verspreiding van de lijsten onder de lidstaten. Hij verwijdert automatisch lijsten overeenkomstig de vervaldata die door de indienende autoriteit voor elke ingediende lijst zijn vermeld.

9. De aangewezen nationale autoriteiten of officiële instanties van de lidstaten die via de gateway persoonsgegevens verwerken, zijn gezamenlijke verwerkingsverantwoordelijken van de verwerkte gegevens. De respectieve verantwoordelijkheden van de gezamenlijke verwerkingsverantwoordelijken worden overeenkomstig bijlage VI toegewezen.

10. De Commissie is de verwerker van de persoonsgegevens die binnen de gateway worden verwerkt. In haar hoedanigheid van verwerker namens de lidstaten zorgt de Commissie voor de beveiliging van de transmissie en de hosting van persoonsgegevens in de gateway en voldoet zij aan de in bijlage VII vastgestelde verplichtingen van de verwerker.

11. De doeltreffendheid van de technische en organisatorische maatregelen om de beveiliging van de verwerking van persoonsgegevens in de gateway te waarborgen, wordt door de Commissie en de gezamenlijke verwerkingsverantwoordelijken regelmatig getest, beoordeeld en geëvalueerd.

Artikel 5 ter

Indiening van lijsten van ingetrokken certificaten door derde landen

Derde landen die COVID-19-certificaten afgeven waarvoor de Commissie krachtens artikel 3, lid 10, of artikel 8, lid 2, van Verordening (EU) 2021/953 een uitvoeringshandeling heeft vastgesteld, kunnen lijsten indienen van ingetrokken COVID-19-certificaten die onder een dergelijke uitvoeringshandeling vallen en die door de Commissie namens de gezamenlijke verwerkingsverantwoordelijken in de in artikel 5 bis bedoelde gateway moeten worden verwerkt, overeenkomstig de technische specificaties in bijlage I.

Artikel 5 quater

Governance van de verwerking van persoonsgegevens in de centrale gateway voor digitale EU-covidcertificaten

1. Het besluitvormingsproces van de gezamenlijke verwerkingsverantwoordelijken wordt geregeld door een werkgroep die is opgericht in het kader van het in artikel 14 van Verordening (EU) 2021/953 bedoelde comité.

2. De aangewezen nationale autoriteiten of officiële instanties van de lidstaten die als gezamenlijke verwerkingsverantwoordelijken via de gateway persoonsgegevens verwerken, wijzen vertegenwoordigers in die groep aan.”.

2) Bijlage I wordt gewijzigd overeenkomstig bijlage I bij dit besluit.

3) Bijlage V wordt gewijzigd overeenkomstig bijlage II bij dit besluit.

4) De tekst in bijlage III bij dit besluit wordt toegevoegd als bijlage VI.

5) De tekst in bijlage IV bij dit besluit wordt toegevoegd als bijlage VII.

Artikel 2

Dit besluit treedt in werking op de derde dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Het is van toepassing met ingang van vier weken na de inwerkingtreding ervan.

Gedaan te Brussel, 21 maart 2022.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

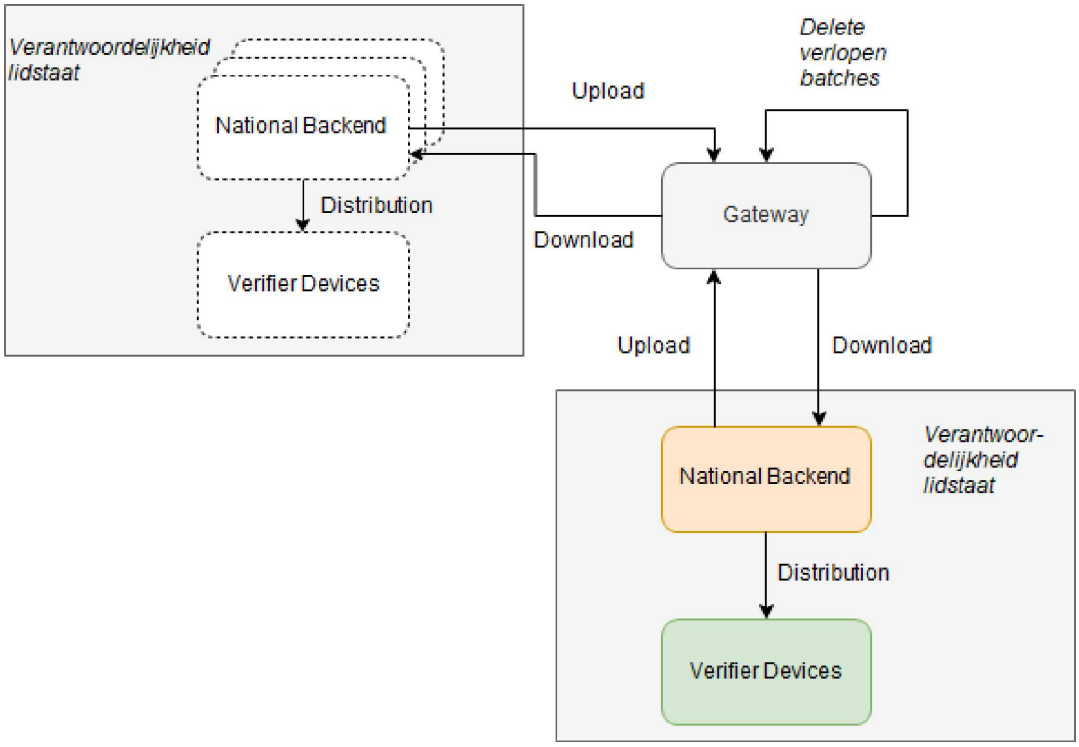
BIJLAGE I

In bijlage I bij Uitvoeringsbesluit (EU) 2021/1073 wordt de volgende afdeling 9 toegevoegd:

"9. **INTREKKINGSOPLOSSING**

9.1. **DCC-intrekkingslijst (DRL)-provision**

De gateway biedt eindpunten ("endpoints") en functies voor het bijhouden en beheren van de intrekkingslijsten:



9.2. **Vertrouwensmodel**

Alle verbindingen komen tot stand via het standaard DCCG-vertrouwensmodel door de NB_{TLS}- en NB_{UP}-certificaten (zie certificaatgovernance). Alle informatie wordt verpakt en geüpload door CMS-berichten om de integriteit te waarborgen.

9.3. **Batch-samenstelling**

9.3.1. *Batch*

Intrekkingslijsten bevatten één of meer vermeldingen en worden verpakt in batches die een reeks hashes en metadata bevatten. Een batch is onveranderlijk ("immutable") en bevat een vervaldatum die aangeeft wanneer de batch kan worden gedeletet. De vervaldatum van alle items in de batch moet exact dezelfde zijn, wat betekent dat de batches moeten worden gegroepeerd per vervaldatum en per ondertekenende DSC (documentondertekenaarscertificaat). Batches bevatten maximaal 1 000 vermeldingen. Als een intrekkingslijst uit meer dan 1 000 vermeldingen bestaat, worden meer batches gemaakt. Een entry mag op hoogstens één batch voorkomen. De batch wordt verpakt in een CMS-structuur en door het NB_{up}-certificaat van het uploadende land ondertekend.

9.3.2. *Batchindex*

Als een batch is aangemaakt, wordt door de gateway een unieke ID toegewezen en wordt die automatisch aan de index toegevoegd. De batchindex wordt gerangschikt op datum van wijziging, in oplopende chronologische volgorde.

9.3.3. *Gateway*

De gateway verwerkt intrekkingsbatches ongewijzigd: bijwerkingen of schrappingen zijn niet mogelijk, noch kan informatie aan de batches worden toegevoegd. De batches worden doorgezonden naar alle bevoegde landen (zie hoofdstuk 9.6).

De gateway monitort de vervaldata van de batches en deletet de vervallen batches. Nadat de batch is gedeletet, meldt de gateway een "HTTP 410 Gone" voor de gedeletete batch URL. De batch verschijnt derhalve in de batchindex als "deleted".

9.4. **Hash types**

De intrekkingslijst bevat hashes die verschillende soorten/attributen van intrekkingen kunnen betekenen. Deze soorten of attributen worden aangegeven bij de opstelling van de intrekkingslijsten. De huidige soorten zijn:

Type	Attribuut	Hash-berekening
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing CountryCode + UCI

Alleen de eerste 128 bits van de hashes die als base64 strings zijn gecodeerd, komen in de batches terecht en worden gebruikt om het ingetrokken DCC te identificeren ([1]).

9.4.1. *Hash type: SHA256(DCC-ondertekening)*

In dit geval wordt de hash berekend aan de hand van de bytes van de COSE_SIGN1-handtekening van de CWT. De formule voor de door de EC-DSA ondertekende certificaten gebruikt de r-waarde als input:

SHA256(r)

[vereist voor alle nieuwe implementaties]

9.4.2. *Hash type: SHA256(UCI)*

In dit geval wordt de hash berekend aan de hand van de bytes van de UCI string die in UTF-8 is gecodeerd en geconverteerd naar een byte array.

[verouderd ([2]), maar ondersteund voor backwards compatibility]

9.4.3. *Hash type: SHA256(Issuing CountryCode+UCI)*

In dit geval wordt de CountryCode gecodeerd als UTF-8 string die met de met een UTF-8 string gecodeerde UCI is samengevoegd. Dit wordt dan geconverteerd naar een byte array en gebruikt als input voor de hashfunctie.

[verouderd[2], maar ondersteund voor backwards compatibility]

9.5. **API-structuur**

9.5.1. *Provisioning API voor intrekkingsvermeldingen*

9.5.1.1. Doel

De API levert de intrekkingslijsten in batches inclusief een batchindex.

9.5.1.2. Eindpunten

([1]) Zie ook 9.5.1.2 voor nadere API-beschrijvingen.
([2]) Verouderd betekent dat deze feature niet in nieuwe implementaties terugkomt, maar voor een bepaalde termijn wordt ondersteund voor nieuwe implementaties.

9.5.1.2.1. Batch List Download Endpoint

De eindpunten volgen een eenvoudig ontwerp, en melden een lijst van batches met een kleine wrapper met metadata. De batches worden gerangschikt op *datum* in *oplopende (chronologische)* volgorde.

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    'more":true|false,
    'batches":
        [{
            'batchId": "{uuid}",
            'country": "XY",
            'date": "2021-11-01T00:00:00Z'
            'deleted": true | false
        }, ..
        ]
}
```

NB: De resultaten worden standaard beperkt tot 1 000. Als de flag "more" op "true" staat, betekent dat dat er meer batches kunnen worden gedownload. Om meer items te downloaden, moet de client de If-Modified-Since header zetten op een datum die niet eerder valt dan de laatst ontvangen vermelding.

Het antwoord bevat een JSON array met de volgende structuur:

Veld	Definitie
more	Boolean Flag die aangeeft dat er meer batches zijn.
batches	Array met de bestaande batches.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Country Code ISO 3166
date	ISO 8601 Date UTC. Datum waarop de batch is toegevoegd of gedeletet.
deleted	Boolean. True indien gedeletet. Als de deleted flag aan staat, kan de entry na zeven dagen definitief uit de query results worden verwijderd.

9.5.1.2.1.1. Response *Codes*

Code	Beschrijving
200	In orde
204	Leeg, als "If-Modified-Since" header content geen match oplevert.

Request Header

Header	Verplicht	Beschrijving
If-Modified-Since	Ja	Deze header bevat de laatst gedownloade datum om de nieuwste resultaten te krijgen. Bij de eerste oproep moet de header op "2021-06-01T00:00:00Z" worden gezet

9.5.1.2.2. Batch Download Endpoint

De batches bevatten een lijst van certificate identifiers:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

'country": "XY",

'expires": "2022-11-01T00:00:00Z",

'kid":"23S+33f=',

'hashType':'SIGNATURE',

'entries":[{

"hash":"e2e2e2e2e2e2e2e2'

}, ..]

}

Het antwoord bevat een CMS met een handtekening die moet overeenkomen met het NB_{UP} -certificaat van het land. Alle items in de JSON array hebben de volgende structuur:

Veld	Verplicht	Type	Definitie
expires	Ja	String	Datum waarop het item kan worden verwijderd. ISO8601 Date/Time UTC
country	Ja	String	Country Code ISO 3166
hashType	Ja	String	Hash Type van de aangeleverde entries (zie Hash Types)
entries	Ja	JSON Object Array	Zie tabel Entries
kid	Ja	String	base64-gecodeerde KID van het DSC dat is gebruikt om het DCC te ondertekenen. Als de KID onbekend is, dan kan de string `UNKNOWN_KID` (zonder de aanhalingstekens) worden gebruikt.

N.B.

— Batches worden gegroepeerd per vervaldatum en per DSC — alle items verstrijken op hetzelfde moment en zijn met dezelfde sleutel ondertekend.

— De vervaltermijn is een datum/tijd in UTC omdat EU-DCC een mondiaal systeem is en een eenduidig tijdstip moet worden gebruikt.

— De vervaldag van een definitief ingetrokken DCC wordt vastgesteld op de vervaldag van het bijbehorende DSC dat is gebruikt om het DCC te ondertekenen, of op de vervaltijd van het ingetrokken DCC (in dat geval worden de gebruikte NumericDate/epoch times beschouwd als in de UTC-tijdzone).

— De National Backend (NB) verwijdert items uit zijn intrekkingslijst als de **vervaldatum** is bereikt.

— De NB kan items uit zijn intrekkingslijst verwijderen als de **kid** die is gebruikt om het DCC te ondertekenen, is ingetrokken.

9.5.1.2.2.1. Entries

Veld	Verplicht	Type	Definitie
hash	Ja	String	De eerste 128 bits van de SHA256 hash, gecodeerd als een base64 string

NB: Het entries object bevat momenteel alleen een hash, maar om compatibel te zijn met toekomstige wijzigingen is gekozen voor een object in plaats van een json array.

9.5.1.2.2.2. Response Codes

Code	Beschrijving
200	In orde
410	Batch weg. Batch kan worden gedeletet in de national backend.

9.5.1.2.2.3. Response Headers

Header	Beschrijving
ETag	Batch ID.

9.5.1.2.3. Batch Upload Endpoint

De upload geschiedt langs hetzelfde eindpunt via POST Verb:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

{

‘country”: “XY”,

‘expires”: “2022-11-01T00:00:00Z”,

‘kid”:„23S+33f=’,

‘hashType”:”SIGNATURE”,

‘entries”:[{

“hash”:”e2e2e2e2e2e2e2e2’

}, ..]

}

De batch wordt ondertekend met het NB_{UP} -certificaat. De gateway controleert of de handtekening door de NB_{UP} is geplaatst voor het betrokken *land*. Als de handtekeningcontrole mislukt, dan gaat de upload niet door.

NB: Iedere batch is immutable en kan na de upload niet worden gewijzigd. Hij kan wel worden gedeletet. De ID van iedere gedeletete batch wordt opgeslagen, en een upload van een nieuwe batch met dezelfde ID wordt geweigerd.

9.5.1.2.4. Batch Delete Endpoint

Een batch kan worden gedeletet langs hetzelfde eindpunt via DELETE Verb:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

‘batchId”: ‘…”

}

of, omwille van de compabiliteit, naar het volgende eindpoint met de POST verb:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

‘batchId”: ‘…”

}

9.6. **API Protection/AVG**

Deze afdeling beschrijft implementatiemaatregelen om te voldoen aan Verordening (EU) 2021/953 inzake de verwerking van persoonsgegevens.

9.6.1. *Bestaande authenticatie*

De gateway gebruikt momenteel het NB_{TLS} -certificaat om de landen te authenticeren die met de gateway verbinden. Deze authenticatie kan worden gebruikt om de identiteit vast te stellen van het land dat met de gateway verbonden is. Die identiteit kan dan worden gebruikt om toegangscontrole te implementeren.

9.6.2. *Toegangscontrole*

Om persoonsgegevens rechtmatig te kunnen verwerken, implementeert de gateway een mechanisme voor toegangscontrole.

De gateway implementeert een Access Control List in combinatie met Role Based Security. In dit kader worden twee tabellen bijgehouden: één tabel waarin wordt beschreven welke rollen welke operations op welke resources kunnen toepassen, en de andere waarin wordt beschreven welke rollen aan welke gebruikers (Users) worden toegewezen.

Drie rollen zijn vereist om de op grond van dit document vereiste controles te implementeren:

RevocationListReader

RevocationUploader

RevocationDeleter

De volgende eindpunten controleren of de gebruiker de rol RevocationListReader heeft; zo ja, dan wordt toegang verleend, anders volgt een HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

De volgende eindpunten controleren of de gebruiker de rol RevocationUploader heeft; zo ja, dan wordt toegang verleend, anders volgt een HTTP 403 Forbidden:

POST/revocation-list

De volgende eindpunten controleren of de gebruiker de rol RevocationDeleter heeft; zo ja, dan wordt toegang verleend, anders volgt een HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

De gateway biedt ook een betrouwbare methode waarmee de beheerders de rollen die aan de gebruikers zijn gekoppeld, zodanig kunnen beheren dat de kans op menselijke fouten wordt beperkt zonder dat de functionele beheerders worden belast.”.

BIJLAGE II

Deel 3 van bijlage V bij Uitvoeringsbesluit (EU) 2021/1073 wordt vervangen door:

"3. ***Gemeenschappelijke structuren en algemene eisen***

Er wordt geen digitaal EU-covidcertificaat afgegeven indien vanwege ontbrekende informatie niet alle datavelden correct kunnen worden ingevuld conform deze specificatie. **Dit doet geen afbreuk aan de verplichting van de lidstaten om digitale EU-covidcertificaten af te geven.**

In alle velden mag informatie worden verstrekt met gebruikmaking van de volledige reeks UNICODE 13.0-tekens die zijn gecodeerd met UTF-8, tenzij dat specifiek beperkt is tot waardereeksen of kleinere reeksen tekens.

De gemeenschappelijke structuur is als volgt:

"JSON":{

"ver":<versie-informatie>,

"nam":{

<persoonnaaminformatie>

},

"dob":<geboortedatum>,

"v" of "t" of "r":[

{<vaccinatiedosis of test of herstelinformatie, één entry>}

]

}

Nadere informatie over de afzonderlijke groepen en velden is te vinden in de volgende hoofdstukken.

Als in de regels is bepaald dat een veld moet worden overgeslagen, houdt dat in dat het leeg is en dat de naam noch de waarde van het veld in de inhoud is toegestaan.

3.1. ***Versie***

Er wordt informatie over de versie verstrekt. De vermelding van versies is gebaseerd op Semantic Versioning (semver: https://semver.org). Tijdens de productie is de versie een van de officieel vrijgegeven versies (huidige versie of een van de oudere versies die officieel zijn vrijgegeven). Zie JSON Schema location voor meer informatie.

ID veld	Naam van het veld	Instructies
ver	Versie schema	Stemt overeen met de identificatiecode van de voor de productie van het EUDCC gebruikte schemaversie. Voorbeeld: "ver":„1.3.0"

3.2. ***Naam en geboortedatum van de persoon***

De naam van de persoon is de officiële volledige naam van de persoon, overeenkomend met de in reisdocumenten vermelde naam. De identificatiecode van de structuur is *nam*. De naam van exact 1 (één) persoon wordt vermeld.

ID veld	Naam van het veld	Instructies
nam/fn	Achternaam/-namen	Achternaam/-namen van de houder Indien de houder geen achternaam maar wel een voornaam heeft, wordt het veld overgeslagen. In alle andere gevallen wordt exact 1 (één) niet-leeg veld vermeld, waarin alle achternamen zijn opgegeven. In het geval van meerdere achternamen worden deze door een spatie gescheiden. Gecombineerde namen met koppeltekens of soortgelijke tekens, moeten echter dezelfde blijven.

		Voorbeelden: “fn”:„Musterfrau-Gößinger” “fn”:„Musterfrau-Gößinger Müller”
nam/fnt	Gestandaardiseerde achternaam/-namen	Achternaam/-namen van de houder, getranslitereerd volgens dezelfde conventie als in de machineleesbare reisdocumenten van de houder (zoals de regels van ICAO Doc 9303 deel 3). Indien de houder geen achternaam maar wel een voornaam heeft, wordt het veld overgeslagen. In alle andere gevallen wordt exact 1 (één) niet-leeg veld vermeld, met uitsluitend de tekens A-Z en <. Maximumlengte: 80 tekens (volgens specificatie ICAO 9303). Voorbeelden: “fnt”:„MUSTERFRAU<GOESSINGER” “fnt”:„MUSTERFRAU<GOESSINGER<MUELLER”
nam/gn	Voornaam/-namen	Voornaam/-namen van de houder. Indien de houder geen voornaam maar wel een achternaam heeft, wordt het veld overgeslagen. In alle andere gevallen wordt exact 1 (één) niet-leeg veld vermeld, waarin alle voornamen zijn opgegeven. In het geval van meerdere voornamen worden deze door een spatie gescheiden. Voorbeeld: “gn”:„Isolde Erika”
nam/gnt	Gestandaardiseerde voornaam/-namen	Voornaam/-namen van de houder, getranslitereerd volgens dezelfde conventie als die welke wordt gebruikt in de machineleesbare reisdocumenten van de houder (zoals de regels van ICAO Doc 9303 deel 3). Indien de houder geen voornaam maar wel een achternaam heeft, wordt het veld overgeslagen. In alle andere gevallen wordt exact 1 (één) niet-leeg veld vermeld, met uitsluitend de tekens A-Z en <. Maximumlengte: 80 tekens. Voorbeeld: “gnt”:„ISOLDE<ERIKA”
dob	Geboortedatum	Geboortedatum van de DCC-houder. Volledige of gedeeltelijke datum zonder tijd, beperkt tot het bereik 1900-01-01 t/m 2099-12-31. Exact 1 (één) niet-leeg veld wordt vermeld indien de volledige of gedeeltelijke geboortedatum bekend is. Indien de geboortedatum zelfs niet gedeeltelijk bekend is, bevat het veld een lege string „”. Die moet overeenkomen met de informatie in de reisdocumenten. Indien er informatie over de geboortedatum beschikbaar is, wordt een van de volgende ISO 8601-formaten gebruikt. Andere opties worden niet ondersteund. JJJJ-MM-DD JJJJ-MM JJJJ (De verificatieapp kan ontbrekende delen van de geboortedatum tonen aan de hand van de XX-conventie zoals die welke wordt gebruikt in machineleesbare reisdocumenten, bv. 1990-XX-XX.) Voorbeelden: “dob”:„1979-04-14” “dob”:„1901-08” “dob”:„1939” “dob”:„”

3.3. ***Groepen voor specifieke informatie betreffende het type certificaat***

Het JSON-schema ondersteunt drie groepen vermeldingen die specifieke informatie betreffende het type certificaat bevatten. Elk EUDCC bevat exact 1 (één) groep. Lege groepen zijn niet toegestaan.

ID groep	Naam groep	Entries
v	Vaccinatiegroep	Bevat, indien aanwezig, exact 1 (één) vermelding die exact 1 (één) vaccinatiedosis (één dosis) beschrijft.
t	Testgroep	Bevat, indien aanwezig, exact 1 (één) vermelding die exact 1 (één) testresultaat beschrijft.
r	Herstelgroep	Bevat, indien aanwezig, exact 1 (één) vermelding die 1 (één) herstelverklaring beschrijft.”

BIJLAGE III

"BIJLAGE VI

VERANTWOORDELIJKHEDEN VAN DE LIDSTATEN ALS GEZAMENLIJKE VERWERKINGSVERANTWOORDELIJKEN VOOR DE GATEWAY VOOR DIGITALE EU-COVIDCERTIFICATEN INZAKE DE UITWISSELING VAN INTREKKINGSLIJSTEN VAN HET EU-DCC

AFDELING 1

Onderafdeling 1

Verdeling van verantwoordelijkheden

(1) De gezamenlijke verwerkingsverantwoordelijken verwerken persoonsgegevens via de vertrouwenskadergateway overeenkomstig de technische specificaties van bijlage I.

(2) De autoriteiten van afgifte van de lidstaten blijven de enige verwerkingsverantwoordelijke voor het verzamelen, het gebruik, de bekendmaking en andere wijzen van verwerking van intrekkingsinformatie buiten de gateway, ook voor de procedure die leidt tot de intrekking van een certificaat.

(3) Iedere verwerkingsverantwoordelijke is verantwoordelijk voor de verwerking van persoonsgegevens in de vertrouwenskadergateway overeenkomstig de artikelen 5, 24 en 26 van de algemene verordening gegevensbescherming.

(4) Iedere verwerkingsverantwoordelijke richt een contactpunt met een functionele mailbox in voor de communicatie tussen de gezamenlijke verwerkingsverantwoordelijken onderling en tussen de gezamenlijke verwerkingsverantwoordelijken en de verwerker.

(5) Een werkgroep die is opgericht door het in artikel 14 van Verordening (EU) 2021/953 bedoelde comité, wordt gemachtigd om zich over alle kwesties uit te spreken die voortvloeien uit de uitwisseling van intrekkingslijsten en uit de gezamenlijke verantwoordelijkheid voor de daarmee samenhangende verwerking van persoonsgegevens, en om gecoördineerde instructies aan de Commissie als verwerker te faciliteren. Het besluitvormingsproces van de gezamenlijke verwerkingsverantwoordelijken wordt geregeld door deze werkgroep en het door haar vast te stellen reglement van orde. Als basisregel geldt dat gezamenlijke verwerkingsverantwoordelijken die niet deelnemen aan een werkgroepvergadering die ten minste zeven dagen van de voren schriftelijk is aangekondigd, stilzwijgend instemmen met de resultaten van die werkgroepvergadering. Iedere gezamenlijke verwerkingsverantwoordelijke kan een vergadering van deze werkgroep bijeenroepen.

(6) Instructies aan de verwerker worden door een van de contactpunten van de gezamenlijke verwerkingsverantwoordelijken in overeenstemming met de andere gezamenlijke verwerkingsverantwoordelijken toegezonden, conform het in punt 5 hierboven beschreven besluitvormingsproces van de werkgroep. De gezamenlijke verwerkingsverantwoordelijke die de instructie geeft, dient deze schriftelijk aan de verwerker te verstrekken en alle andere gezamenlijke verwerkingsverantwoordelijken hiervan in kennis te stellen. Als een zaak onder zodanige tijdsdruk staat dat er geen vergadering van de werkgroep conform punt 5 kan plaatsvinden, kan er toch een instructie worden gegeven, maar die kan door de werkgroep worden herroepen. De instructie moet schriftelijk worden gegeven, en alle andere gezamenlijke verwerkingsverantwoordelijken moeten op het moment van het geven van de instructie daarvan op de hoogte worden gesteld.

(7) De conform punt 5 ingestelde werkgroep laat de individuele bevoegdheid van de gezamenlijke verwerkingsverantwoordelijken onverlet om hun bevoegde toezichthoudende autoriteiten overeenkomstig de artikelen 33 en 24 van de algemene verordening gegevensbescherming in te lichten. Voor deze melding is de instemming van de andere gezamenlijke verwerkingsverantwoordelijken niet vereist.

(8) In het kader van de vertrouwenskadergateway mogen alleen daartoe door de aangewezen nationale autoriteiten of officiële instanties gemachtigde personen toegang krijgen tot de uitgewisselde persoonsgegevens.

(9) Iedere autoriteit van afgifte houdt een register bij van de verwerkingsactiviteiten die onder haar verantwoordelijkheid plaatsvinden. De gezamenlijke verwerkingsverantwoordelijkheid mag in het register worden vermeld.

Onderafdeling 2

Verantwoordelijkheden en rollen voor het behandelen van verzoeken en voor het informeren van betrokkenen

1) Iedere verwerkingsverantwoordelijke verstrekt de natuurlijke personen wier certificaat of certificaten hij heeft ingetrokken ("de betrokkenen") in zijn rol van autoriteit van afgifte informatie over die intrekking en de verwerking van hun persoonsgegevens in de gateway voor digitale EU-covidcertificaten ter ondersteuning van de uitwisseling van intrekkingslijsten, overeenkomstig artikel 14 van de algemene verordening gegevensbescherming, tenzij dit onmogelijk blijkt of onevenredig veel moeite kost.

2) Iedere verwerkingsverantwoordelijke treedt op als contactpunt voor natuurlijke personen wier certificaat hij heeft ingetrokken en behandelt de verzoeken die betrokkenen of hun vertegenwoordigers in het kader van de uitoefening van hun rechten overeenkomstig de algemene verordening gegevensbescherming indienen. Indien een gezamenlijke verwerkingsverantwoordelijke een verzoek van een betrokkene ontvangt dat betrekking heeft op een door een andere gezamenlijke verwerkingsverantwoordelijke afgegeven certificaat, stelt hij de betrokkene in kennis van de identiteit en de contactgegevens van die verantwoordelijke gezamenlijke verwerkingsverantwoordelijke. De gezamenlijke verwerkingsverantwoordelijken verlenen elkaar op onderling verzoek bijstand bij het behandelen van de verzoeken van de betrokkenen en beantwoorden elkaar onverwijld, en uiterlijk binnen één maand na ontvangst van een verzoek om bijstand. Indien een verzoek verband houdt met door een derde land ingediende gegevens, behandelt de verwerkingsverantwoordelijke het verzoek en stelt hij de betrokkene in kennis van de identiteit en de contactgegevens van de autoriteit van afgifte in het derde land.

3) Iedere verwerkingsverantwoordelijke stelt de inhoud van deze bijlage, met inbegrip van de in de punten 1 en 2 vastgestelde regelingen, ter beschikking van de betrokkene.

AFDELING 2

Beheer van beveiligingsincidenten, met inbegrip van inbreuken in verband met persoonsgegevens

1) De gezamenlijke verwerkingsverantwoordelijken verlenen elkaar bijstand bij de identificatie en behandeling van beveiligingsincidenten, met inbegrip van inbreuken in verband met persoonsgegevens, die verband houden met de verwerking in de gateway voor digitale EU-covidcertificaten.

2) De gezamenlijke verwerkingsverantwoordelijken stellen elkaar met name in kennis van:
   a) alle potentiële of feitelijke risico's voor de beschikbaarheid, de vertrouwelijkheid en/of de integriteit van de persoonsgegevens die in de vertrouwenskadergateway worden verwerkt;
   b) alle inbreuken in verband met persoonsgegevens, de waarschijnlijke gevolgen van die inbreuken en de beoordeling van het risico voor de rechten en vrijheden van natuurlijke personen, alsmede alle maatregelen die zijn genomen om de inbreuken in verband met persoonsgegevens aan te pakken en het risico voor de rechten en vrijheden van natuurlijke personen te beperken;
   c) alle inbreuken op de technische en/of organisatorische waarborgen van de verwerking in de vertrouwenskadergateway.

3) De gezamenlijke verwerkingsverantwoordelijken melden, overeenkomstig de artikelen 33 en 34 van de algemene verordening gegevensbescherming of na kennisgeving door de Commissie, alle inbreuken in verband met de verwerking in de vertrouwenskadergateway aan de Commissie, aan de bevoegde toezichthoudende autoriteiten en, in voorkomend geval, aan de betrokkenen.

4) Iedere autoriteit van afgifte neemt passende technische en organisatorische maatregelen om:
   a) de beschikbaarheid, de integriteit en de vertrouwelijkheid van de gezamenlijk verwerkte persoonsgegevens te waarborgen en te beschermen;
   b) persoonsgegevens in haar bezit te beschermen tegen ongeoorloofde of onrechtmatige verwerking, verlies, gebruik, openbaarmaking, verkrijging of toegang;
   c) te waarborgen dat de persoonsgegevens niet algemeen toegankelijk zijn of toegankelijk zijn voor anderen dan de ontvangers of verwerkers.

AFDELING 3

Gegevensbeschermingseffectbeoordeling

1) Indien een verwerkingsverantwoordelijke, om te voldoen aan zijn verplichtingen uit hoofde van de artikelen 35 en 36 van Verordening (EU) 2016/679, informatie van een andere verwerkingsverantwoordelijke nodig heeft, zendt hij een specifiek verzoek naar de in afdeling 1, onderafdeling 1, punt 4, bedoelde functionele mailbox. De laatstgenoemde zal alles in het werk stellen om deze informatie te verstrekken."

BIJLAGE IV

"BIJLAGE VII

VERANTWOORDELIJKHEDEN VAN DE COMMISSIE ALS GEGEVENSVERWERKER VOOR DE GATEWAY VOOR DIGITALE EU-COVIDCERTIFICATEN TER ONDERSTEUNING VAN DE UITWISSELING VAN INTREKKINGSLIJSTEN VAN HET EU-DCC

De Commissie:

1) bewerkstelligt en waarborgt namens de lidstaten een beveiligde en betrouwbare communicatie-infrastructuur ter ondersteuning van de uitwisseling van intrekkingslijsten die bij de gateway voor digitale EU-covidcertificaten zijn ingediend;

2) kan, om haar verplichtingen als gegevensverwerker van de vertrouwenskadergateway voor de lidstaten na te komen, derden als subverwerkers inschakelen; licht de verwerkingsverantwoordelijken in over beoogde veranderingen inzake de toevoeging of vervanging van andere subverwerkers, en zo de verwerkingsverantwoordelijken de mogelijkheid bieden gezamenlijk tegen deze veranderingen bezwaar te maken. De Commissie zorgt ervoor dat dezelfde verplichtingen inzake gegevensbescherming als uiteengezet in dit besluit van toepassing zijn op deze subverwerkers;

3) verwerkt de persoonsgegevens uitsluitend op basis van schriftelijke instructies van de verwerkingsverantwoordelijken, tenzij een Unierechtelijke of lidstaatrechtelijke bepaling haar tot verwerking verplicht; in dat geval stelt de Commissie de gezamenlijke verwerkingsverantwoordelijken, voorafgaand aan de uitvoering van de verwerkingsactiviteit, in kennis van dat wettelijk voorschrift, tenzij die wetgeving kennisgeving van dergelijke informatie om gewichtige redenen van algemeen belang verbiedt;

   verwerkt de gegevens als volgt:

   a) authenticatie van nationale backendservers, op basis van nationale backendservercertificaten;

   b) ontvangst van de in artikel 5 bis, lid 3, van het besluit bedoelde gegevens die door nationale achtergrondservers zijn geüpload door te voorzien in een applicatieprogramma-interface die nationale backendservers in staat stelt de relevante gegevens te uploaden;

   c) opslag van de gegevens in de gateway voor digitale EU-covidcertificaten;

   d) beschikbaar stellen van de gegevens om door de nationale achtergrondservers te worden gedownload;

   e) verwijdering van de gegevens op de vervaldatum of in opdracht van de verwerkingsverantwoordelijke die ze heeft ingediend;

   f) na de beëindiging van de dienstverlening, wissen van alle resterende gegevens, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk verplicht is;

4) neemt alle geavanceerde organisatorische, fysieke en logische beveiligingsmaatregelen om de gateway voor digitale EU-covidcertificaten in stand te houden. Hiertoe zal de commissie:

   a) een verantwoordelijke entiteit aanwijzen voor de gateway voor digitale EU-covidcertificaten, de gezamenlijke verwerkingsverantwoordelijken in kennis stellen van de contactgegevens van de entiteit en ervoor zorgen dat deze beschikbaar is om te reageren op bedreigingen voor de beveiliging;

   b) de verantwoordelijkheid voor de beveiliging van de gateway voor digitale EU-covidcertificaten op zich nemen, onder meer door regelmatig tests, evaluaties en beoordelingen van de beveiligingsmaatregelen uit te voeren;

   c) ervoor zorgen dat alle personen aan wie toegang tot de gateway voor digitale EU-covidcertificaten is verleend, onderworpen zijn aan een contractuele, professionele of wettelijke verplichting tot vertrouwelijkheid;

5) neemt alle nodige veiligheidsmaatregelen om te voorkomen dat de goede werking van nationale backendservers in het gedrang komt. Daartoe voert de Commissie specifieke procedures in met betrekking tot de verbinding van de backendservers naar de gateway voor digitale EU-covidcertificaten. Die bestaan uit:

   a) een risicobeoordelingsprocedure om potentiële bedreigingen van het systeem te identificeren en in te schatten;

   b) een audit- en evaluatieprocedure om:

      i) de overeenstemming tussen de uitgevoerde beveiligingsmaatregelen en het toepasselijke beveiligingsbeleid te controleren;

      ii) regelmatig de integriteit van de systeembestanden, de beveiligingsparameters en de verleende machtigingen te controleren;

iii) toezicht te houden teneinde beveiligingsinbreuken te identificeren;

iv) wijzigingen door te voeren om bestaande zwakke punten in de beveiliging te remediëren;

v) de voorwaarden vast te stellen voor het toestaan, onder meer op verzoek van verwerkingsverantwoordelijken, van en het leveren van een bijdrage aan de uitvoering van onafhankelijke audits, met inbegrip van inspecties, en evaluaties van de veiligheidsmaatregelen, onder voorwaarden die Protocol nr. 7 bij het VWEU betreffende de voorrechten en immuniteiten van de Europese Unie in acht nemen;

c) wijziging van de beheersprocedure om de gevolgen van een wijziging vóór de uitvoering ervan te documenteren en te meten, en de gezamenlijke verwerkingsverantwoordelijken op de hoogte houden van wijzigingen die van invloed kunnen zijn op de communicatie met en/of de beveiliging van hun infrastructuren;

d) vaststelling van een onderhouds- en reparatieprocedure om de na te leven regels en voorwaarden voor het onderhoud en/of het repareren van apparatuur te specificeren;

e) vaststelling van een procedure voor beveiligingsincidenten om het meldings- en escalatiesysteem vast te stellen, de getroffen verwerkingsverantwoordelijken onverwijld in kennis te stellen, de verwerkingsverantwoordelijken onverwijld in kennis te stellen zodat zij de nationale toezichthoudende autoriteiten voor gegevensbescherming op de hoogte kunnen brengen van eventuele inbreuken in verband met persoonsgegevens, en een disciplinair proces vast te stellen om inbreuken op de beveiliging aan te pakken;

6) neemt geavanceerde materiële en/of logische veiligheidsmaatregelen voor de installaties waar de apparatuur van de gateway voor digitale EU-covidcertificaten is ondergebracht en voor controles met betrekking tot de toegang tot logische gegevens en beveiliging. Hiertoe zal de commissie:

a) fysieke beveiliging handhaven om afzonderlijke veiligheidszones op te stellen en de opsporing van inbreuken mogelijk te maken;

b) de toegang tot de faciliteiten controleren en met het oog op de traceerbaarheid een register van bezoekers bijhouden;

c) ervoor zorgen dat externe personen die toegang krijgen tot gebouwen, worden begeleid door naar behoren gemachtigd personeel;

d) ervoor zorgen dat apparatuur niet kan worden toegevoegd, vervangen of verwijderd zonder voorafgaande machtiging van de aangewezen verantwoordelijke instanties;

e) de wederzijdse toegang van en tot de nationale backendservers en de vertrouwenskadergateway controleren;

f) ervoor zorgen dat personen die toegang hebben tot de gateway voor digitale EU-covidcertificaten geïdentificeerd en geauthenticeerd worden;

g) de machtiging met betrekking tot de toegang tot de gateway voor digitale EU-covidcertificaten herzien in geval van een inbreuk op de beveiliging die gevolgen heeft voor deze infrastructuur;

h) de integriteit van de via de gateway voor digitale EU-covidcertificaten doorgegeven informatie bewaren;

i) technische en organisatorische veiligheidsmaatregelen ten uitvoer leggen om ongeoorloofde toegang tot persoonsgegevens te voorkomen;

j) waar nodig maatregelen treffen om ongeoorloofde toegang tot de gateway voor digitale EU-covidcertificaten vanaf het domein van de nationale autoriteiten te blokkeren (dat wil zeggen: een locatie/IP-adres blokkeren);

7) onderneemt stappen om haar domein te beschermen, met inbegrip van het verbreken van verbindingen, in geval van een aanzienlijke afwijking van de kwaliteits- of beveiligingsbeginselen en -concepten;

8) houdt een risicobeheerplan in stand dat betrekking heeft op het gebied waarvoor zij verantwoordelijk is;

9) monitort — in real time — de prestaties van alle dienstencomponenten van de diensten van haar vertrouwenskadergateway, produceert regelmatig statistieken en registreert gegevens;

10) ondersteunt continu alle diensten van de vertrouwenskadergateway in het Engels via telefoon, mail of webportal en accepteert oproepen van geautoriseerde oproepers: de coördinatoren van de gateway voor digitale EU-covidcertificaten en hun respectieve helpdesks, projectmedewerkers en aangewezen personen van de Commissie;

11) staat, voor zover mogelijk overeenkomstig artikel 12 van Verordening (EU) 2018/1725, de gezamenlijke verwerkingsverantwoordelijken door middel van passende technische en organisatorische maatregelen bij in de naleving van hun verplichting om te antwoorden op verzoeken tot uitoefening van de rechten van betrokkenen, zoals vastgesteld in hoofdstuk III van de algemene verordening gegevensbescherming;

12) ondersteunt de gezamenlijke verwerkingsverantwoordelijken door informatie te verstrekken over de gateway voor digitale EU-covidcertificaten, teneinde de verplichtingen uit hoofde van de artikelen 32, 33, 34, 35 en 36 van de algemene verordening gegevensbescherming na te leven;

13) zorgt ervoor dat de gegevens die binnen de gateway voor digitale EU-covidcertificaten worden verwerkt, onbegrijpelijk zijn voor onbevoegden;

14) neemt alle nodige maatregelen om te voorkomen dat de gebruikers van de gateway voor digitale EU-covidcertificaten ongeoorloofd toegang hebben tot doorgegeven gegevens;

15) neemt maatregelen om de interoperabiliteit en de communicatie tussen de verwerkingsverantwoordelijken voor de gateway voor digitale EU-covidcertificaten te bevorderen;

16) houdt overeenkomstig artikel 31, lid 2, van Verordening (EU) 2018/1725 een register bij van de verwerkingsactiviteiten die ten behoeve van de gezamenlijke verwerkingsverantwoordelijken zijn verricht.”.