II

(Niet-wetgevingshandelingen)

BESLUITEN

UITVOERINGSBESLUIT (EU) 2020/1023 VAN DE COMMISSIE

van 15 juli 2020

tot wijziging van Uitvoeringsbesluit (EU) 2019/1765 wat betreft de grensoverschrijdende uitwisseling van gegevens tussen nationale mobiele applicaties voor het traceren en waarschuwen van contacten met het oog op de bestrijding van de COVID-19-pandemie

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg ([1]), en met name artikel 14, lid 3,

Overwegende hetgeen volgt:

(1) In artikel 14 van Richtlijn 2011/24/EU is bepaald dat de Unie de samenwerking en de uitwisseling van informatie tussen de lidstaten steunt en bevordert in het kader van een vrijwillig netwerk waarin de door de lidstaten aangewezen nationale autoriteiten die verantwoordelijk zijn voor e-gezondheid (eHealth) met elkaar worden verbonden (het "e-gezondheidsnetwerk").

(2) Bij Uitvoeringsbesluit (EU) 2019/1765 van de Commissie ([2]) zijn de voorschriften voor de oprichting, het beheer en de werking van het netwerk van nationale verantwoordelijke autoriteiten inzake e-gezondheid vastgesteld. Krachtens artikel 4 van dat besluit heeft het e-gezondheidsnetwerk tot taak de interoperabiliteit van de nationale systemen voor informatie- en communicatietechnologie en de grensoverschrijdende overdraagbaarheid van elektronische gezondheidsgegevens bij grensoverschrijdende gezondheidszorg te bevorderen.

(3) In het licht van de door de COVID-19-pandemie veroorzaakte volksgezondheidscrisis hebben meerdere lidstaten mobiele applicaties ontwikkeld die contacttracering ondersteunen en waarmee de gebruikers van dergelijke applicaties zich kunnen laten waarschuwen om passende maatregelen te nemen, zoals zich laten testen of in zelfisolatie gaan, als zij mogelijk aan het virus zijn blootgesteld door de nabijheid van een andere gebruiker van een dergelijke applicatie die een positieve diagnose heeft gemeld. Deze applicaties maken gebruik van bluetooth-technologie om te detecteren dat toestellen zich in elkaars nabijheid bevinden. Aangezien de beperkingen op het reizen tussen de lidstaten sinds juni 2020 zijn opgeheven, moet een betere interoperabiliteit van de nationale systemen voor informatie- en communicatietechnologie tussen de lidstaten die deelnemen aan het e-gezondheidsnetwerk tot stand worden gebracht door middel van de invoering van een digitale infrastructuur die de interoperabiliteit tussen de nationale mobiele applicaties ter ondersteuning van het traceren en waarschuwen van contacten mogelijk maakt.

([1]) PB L 88 van 4.4.2011, blz. 45.

([2]) Uitvoeringsbesluit (EU) 2019/1765 van de Commissie van 22 oktober 2019 tot vaststelling van de voorschriften voor de oprichting, het beheer en de werking van het netwerk van nationale autoriteiten die verantwoordelijk zijn voor e-gezondheid, en tot intrekking van Uitvoeringsbesluit 2011/890/EU (PB L 270 van 24.10.2019, blz. 83).

(4) De Commissie ondersteunt de lidstaten met betrekking tot de bovengenoemde mobiele applicaties. Op 8 april 2020 heeft de Commissie een aanbeveling aangenomen over een gemeenschappelijke toolbox van de Unie voor het gebruik van technologie en gegevens om de COVID-19-crisis te bestrijden en te boven te komen, met name wat mobiele applicaties en het gebruik van geanonimiseerde mobiliteitsgegevens betreft (de "aanbeveling van de Commissie") ([3]). Met de steun van de Commissie hebben de lidstaten die deelnemen aan het e-gezondheidsnetwerk een gemeenschappelijke EU-toolbox voor de lidstaten op het gebied van mobiele applicaties ter ondersteuning van contacttracering ([4]) en richtsnoeren voor interoperabiliteit voor goedgekeurde mobiele contacttraceringsapplicaties in de EU ([5]) vastgesteld. De toolbox bevat uitleg over de nationale vereisten voor de nationale mobiele applicaties voor het traceren en waarschuwen van contacten, in het bijzonder over het feit dat het gebruik ervan op vrijwillig basis moet berusten, dat zij door de respectieve nationale gezondheidsautoriteiten moeten zijn goedgekeurd, dat zij de privacy moeten beschermen, en dat zij moeten worden verwijderd zodra zij niet meer nodig zijn. Naar aanleiding van de recentste ontwikkelingen in de COVID-19-crisis hebben zowel de Commissie ([6]) als het Europees Comité voor gegevensbescherming ([7]) advies uitgebracht over mobiele applicaties en instrumenten voor contacttracering wat betreft de gegevensbescherming. Het ontwerp van de mobiele applicaties van de lidstaten en van de digitale infrastructuur die hun interoperabiliteit mogelijk maakt, bouwt voort op de gemeenschappelijke EU-toolbox, de bovengenoemde richtsnoeren en de technische specificaties die in het kader van het e-gezondheidsnetwerk zijn overeengekomen.

(5) Om de interoperabiliteit van nationale mobiele applicaties voor het traceren en waarschuwen van contacten te bevorderen, is met de steun van de Commissie door de lidstaten die deelnemen aan het e-gezondheidsnetwerk en die hebben besloten hun samenwerking op dit gebied op vrijwillige basis te intensifiëren, een digitale infrastructuur ontwikkeld, in de vorm van een IT-instrument voor de uitwisseling van gegevens. Deze digitale infrastructuur wordt "de federatieve gateway" genoemd.

(6) Dit besluit bevat bepalingen over de rol van de deelnemende lidstaten en van de Commissie voor de werking van de federatieve gateway voor de grensoverschrijdende interoperabiliteit van nationale mobiele applicaties voor het traceren en waarschuwen van contacten.

(7) De verwerking van persoonsgegevens van de applicatiegebruikers van mobiele applicaties voor het traceren en waarschuwen van contacten, die onder de verantwoordelijkheid van de lidstaten of andere publieke organisaties of officiële instanties in de lidstaten plaatsvindt, moet worden uitgevoerd in overeenstemming met Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([8]) ("de algemene verordening gegevensbescherming") en Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([9]). De verwerking van persoonsgegevens onder de verantwoordelijkheid van de Commissie met het oog op het beheer en de waarborging van de beveiliging van de federatieve gateway moet in overeenstemming zijn met Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([10]).

(8) De federatieve gateway moet bestaan uit een beveiligde IT-infrastructuur bieden die voorziet in een gemeenschappelijke interface waar aangewezen nationale autoriteiten of officiële instanties een minimale verzameling gegevens kunnen uitwisselen over de contacten met personen die met SARS-CoV-2 zijn besmet, teneinde anderen te informeren over hun mogelijke blootstelling aan die besmetting, en die de doeltreffende samenwerking tussen de lidstaten op het gebied van gezondheidszorg bevordert door de uitwisseling van relevante informatie te vergemakkelijken.

(9) In dit besluit moeten derhalve regels worden vastgesteld voor de grensoverschrijdende uitwisseling van gegevens tussen aangewezen nationale autoriteiten of officiële instanties via de federatieve gateway binnen de EU.

([3]) Aanbeveling (EU) 2020/518 van de Commissie van 8 april 2020 over een gemeenschappelijke toolbox voor het gebruik van technologie en gegevens om de COVID-19-crisis te bestrijden en te boven te komen, met name wat mobiele applicaties en het gebruik van geanonimiseerde mobiliteitsgegevens betreft (PB L 114 van 14.4.2020, blz. 7).

([4]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

([5]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

([6]) Mededeling van de Commissie — Richtsnoeren in verband met gegevensbescherming voor apps ter ondersteuning van de bestrijding van de COVID-19-pandemie (PB C 124I van 17.4.2020, blz. 1).

([7]) Richtsnoeren 04/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19 en de verklaring van het Europees Comité voor gegevensbescherming van 16 juni 2020 over de gevolgen van de interoperabiliteit van contacttraceringsapps voor gegevensbescherming, beide beschikbaar op: https://edpb.europa.eu

([8]) 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).

([9]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

([10]) 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).

(10) De deelnemende lidstaten, vertegenwoordigd door de aangewezen nationale autoriteiten of officiële instanties, bepalen gezamenlijk de doeleinden en middelen van de verwerking van persoonsgegevens via de federatieve gateway en zijn derhalve gezamenlijke verwerkingsverantwoordelijken. Op grond van artikel 26 van de algemene verordening gegevensbescherming 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 verwerkingsverantwoordelijken moeten ervoor zorgen dat zij over een rechtsgrond op nationaal niveau beschikken voor de verwerking in de federatieve gateway.

(11) De Commissie, als aanbieder van technische en organisatorische oplossingen voor de federatieve gateway, verwerkt gepseudonimiseerde persoonsgegevens namens de lidstaten die als gezamenlijke verwerkingsverantwoordelijken deelnemen aan de federatieve gateway en is derhalve een verwerker. Krachtens artikel 28 van de algemene verordening gegevensbescherming en artikel 29 van Verordening (EU) 2018/1725 wordt de verwerking door een verwerker geregeld in een overeenkomst of een rechtshandeling krachtens het Unierecht of het lidstatelijke recht die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt en de verwerking specificeert. In dit besluit worden de regels vastgesteld voor de verwerking door de Commissie als verwerker.

(12) Bij de verwerking van persoonsgegevens in het kader van de federatieve gateway is de Commissie gebonden door Besluit (EU, Euratom) 2017/46 van de Commissie ([11]).

(13) Aangezien de doeleinden waarvoor de verwerkingsverantwoordelijken persoonsgegevens verwerken in de nationale mobiele applicaties voor het traceren en waarschuwen van contacten niet noodzakelijkerwijs de identificatie van een betrokkene vereisen, zijn de verwerkingsverantwoordelijken mogelijk niet altijd in staat de toepassing van de rechten van betrokkenen te waarborgen. De in de artikelen 15 tot en met 20 van de algemene verordening gegevensbescherming bedoelde rechten zijn derhalve mogelijk niet van toepassing indien aan de voorwaarden van artikel 11 van die verordening is voldaan.

(14) De bestaande bijlage bij Uitvoeringsbesluit (EU) 2019/1765 moet worden hernummerd als gevolg van de toevoeging van twee nieuwe bijlagen.

(15) Uitvoeringsbesluit (EU) 2019/1765 moet daarom dienovereenkomstig worden gewijzigd.

(16) Gezien de urgentie van de door de COVID-19-pandemie veroorzaakte situatie moet dit besluit van toepassing zijn met ingang van de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

(17) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 en heeft op 9 juli 2020 advies uitgebracht.

(18) De in dit besluit vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 16 van Richtlijn 2011/24/EU ingestelde comité,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Uitvoeringsbesluit (EU) 2019/1765 wordt als volgt gewijzigd:

1) In artikel 2, lid 1, worden de volgende punten g), h), i), j), k), l), m), n) en o) toegevoegd:

"g) "applicatiegebruiker": een persoon die in het bezit is van een slim apparaat en die een goedgekeurde mobiele applicatie voor het traceren en waarschuwen van contacten heeft gedownload en deze uitvoert;

h) "contacttracering" of "traceren van contacten": maatregelen om personen te traceren die zijn blootgesteld aan een bron van een ernstige grensoverschrijdende bedreiging van de gezondheid in de zin van artikel 3, onder c), van Besluit nr. 1082/2013/EU van het Europees Parlement en de Raad (*);

([11]) Besluit (EU, Euratom) 2017/46 van de Commissie van 10 januari 2017 over de beveiliging van communicatie- en informatiesystemen binnen de Europese Commissie (PB L 6 van 11.1.2017, blz. 40). 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

i) "nationale mobiele applicatie voor het traceren en waarschuwen van contacten": een op nationaal niveau goedgekeurde softwareapplicatie die draait op slimme apparaten, met name smartphones, die gewoonlijk zijn ontworpen voor een brede en gerichte interactie met internetbronnen, en die nabijheidsgegevens en andere contextuele informatie uit de vele sensoren in de slim apparaten verwerkt met het oog op het traceren van contacten met personen die besmet zijn met SARS-CoV-2 en het waarschuwen van personen die mogelijk aan SARS-CoV-2 zijn blootgesteld. Deze mobiele applicaties kunnen de aanwezigheid van andere apparaten detecteren met behulp van bluetooth en informatie uitwisselen met backendservers via het internet;

j) "federatieve gateway": een netwerkgateway die door de Commissie wordt beheerd door middel van een beveiligd IT-instrument dat een minimale verzameling persoonsgegevens ontvangt, opslaat en beschikbaar stelt tussen de backendservers van de lidstaten, met als doel de interoperabiliteit van de nationale mobiele applicaties voor het traceren en waarschuwen van contacten te waarborgen;

k) "sleutel": een unieke kortstondige identificatiecode die gerelateerd is aan een applicatiegebruiker die meldt met SARS-CoV-2 te zijn besmet of die mogelijk aan SARS-CoV-2 is blootgesteld;

l) "verificatie van de besmetting": de methode die is toegepast om een besmetting met SARS-CoV-2 te bevestigen, d.w. z. melding door de applicatiegebruiker zelf of bevestiging door een nationale gezondheidsautoriteit of een laboratoriumtest;

m) "relevante landen": de lidstaat of lidstaten waar een applicatiegebruiker zich in de laatste 14 dagen vóór de datum van het uploaden van de sleutels heeft bevonden, waar deze de goedgekeurde nationale mobiele applicatie voor het traceren en waarschuwen van contacten heeft gedownload, en/of waar deze heeft gereisd;

n) "land van oorsprong van de sleutels": de lidstaat waar de backendserver die de sleutels heeft geüpload naar de federatieve gateway, zich bevindt;

o) "loggegevens": een automatische registratie van een activiteit in verband met de uitwisseling van en toegang tot gegevens die via de federatieve gateway zijn verwerkt, waaruit met name het soort verwerkingsactiviteit, de datum en het tijdstip van de verwerkingsactiviteit en de identificatiecode van de persoon die de gegevens verwerkt, blijken.

(*) Besluit nr. 1082/2013/EU van het Europees Parlement en de Raad van 22 oktober 2013 over ernstige grensoverschrijdende bedreigingen van de gezondheid en houdende intrekking van Beschikking nr. 2119/98/EG (PB L 293 van 5.11.2013, blz. 1).".

2) In artikel 4, lid 1, wordt het volgende punt h) toegevoegd:

"h) de lidstaten richtsnoeren vertrekken over de grensoverschrijdende uitwisseling van persoonsgegevens via de federatieve gateway tussen nationale mobiele applicaties voor het traceren en waarschuwen van contacten.".

3) In artikel 6, lid 1, worden de volgende punten f) en g) toegevoegd:

"f) ontwikkelt, implementeert en onderhoudt passende technische en organisatorische maatregelen met betrekking tot de beveiliging van de doorgifte en hosting van persoonsgegevens in de federatieve gateway, teneinde de interoperabiliteit van nationale mobiele applicaties voor het traceren en waarschuwen van contacten te waarborgen;

g) ondersteunt het e-gezondheidsnetwerk bij het bereiken van overeenstemming over de technische en organisatorische naleving door de nationale autoriteiten van de vereisten voor de grensoverschrijdende uitwisseling van persoonsgegevens in de federatieve gateway door het verstrekken en uitvoeren van de nodige tests en audits. De auditoren van de Commissie kunnen worden bijgestaan door deskundigen uit de lidstaten.".

4) Artikel 7 wordt als volgt gewijzigd:

a) de titel wordt vervangen door "Bescherming van persoonsgegevens die worden verwerkt via de digitale diensteninfrastructuur voor e-gezondheid";

b) in lid 2 worden de woorden "de bijlage" vervangen door "bijlage I".

5) Het volgende artikel 7 bis wordt ingevoegd:

"*Artikel 7 bis*

Grensoverschrijdende uitwisseling van gegevens tussen nationale mobiele applicaties voor het traceren en waarschuwen van contacten via de federatieve gateway

1. Wanneer persoonsgegevens via de federatieve gateway worden uitgewisseld, worden deze uitsluitend verwerkt om de interoperabiliteit van nationale mobiele applicaties voor het traceren en waarschuwen van contacten binnen de federatieve gateway en de continuïteit van de contacttracering in een grensoverschrijdende context te bevorderen.

2. De in lid 3 bedoelde persoonsgegevens worden in een gepseudonimiseerd formaat aan de federatieve gateway doorgegeven.

3. De gepseudonimiseerde persoonsgegevens die uitgewisseld worden via en verwerkt worden in de federatieve gateway omvatten uitsluitend de volgende informatie:

a) de sleutels die tot 14 dagen vóór de datum van het uploaden van de sleutels zijn doorgegeven door de nationale mobiele applicaties voor het traceren en waarschuwen van contacten;

b) loggegevens inzake de sleutels, overeenkomstig het in het land van oorsprong van de sleutels toegepaste protocol voor de technische specificaties;

c) de verificatie van de besmetting;

d) de relevante landen en het land van oorsprong van de sleutels.

4. De aangewezen nationale autoriteiten of officiële instanties die persoonsgegevens verwerken in de federatieve gateway zijn gezamenlijke verwerkingsverantwoordelijken met betrekking tot de in de federatieve gateway verwerkte gegevens. De respectieve verantwoordelijkheden van de gezamenlijke verwerkingsverantwoordelijken worden overeenkomstig bijlage II toegewezen. Elke lidstaat die wenst deel te nemen aan de grensoverschrijdende uitwisseling van gegevens tussen nationale mobiele applicaties voor het traceren en waarschuwen van contacten, stelt de Commissie vooraf van dit voornemen in kennis en geeft aan welke nationale autoriteit of officiële instantie als verwerkingsverantwoordelijke is aangewezen.

5. De Commissie is de verwerker van de persoonsgegevens die binnen de federatieve gateway worden verwerkt. In haar hoedanigheid van verwerker draagt de Commissie zorg voor de beveiliging van de verwerking, met inbegrip van de doorgifte en hosting, van persoonsgegevens in de federatieve gateway, en voldoet zij aan de in bijlage III vastgestelde verplichtingen van een verwerker.

6. De doeltreffendheid van de technische en organisatorische maatregelen om de beveiliging van de verwerking van persoonsgegevens binnen de federatieve gateway te waarborgen, wordt regelmatig getest, beoordeeld en geëvalueerd door de Commissie en door de nationale autoriteiten die toegang hebben tot de federatieve gateway.

7. Onverminderd het besluit van de gezamenlijke verwerkingsverantwoordelijken om de verwerking in de federatieve gateway te beëindigen, wordt de federatieve gateway uiterlijk 14 dagen nadat alle verbonden nationale mobiele applicaties voor het traceren en waarschuwen van contacten zijn opgehouden sleutels via de federatieve gateway door te geven, gedeactiveerd.".

6) De bijlage wordt bijlage I.

7) De bijlagen II en III, waarvan de tekst is opgenomen in de bijlage bij dit besluit, worden toegevoegd.

Artikel 2

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

Gedaan te Brussel, 15 juli 2020.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE

Aan Uitvoeringsbesluit (EU) 2019/1765 worden de volgende bijlagen II en III toegevoegd:

"BIJLAGE II

VERANTWOORDELIJKHEDEN VAN DE DEELNEMENDE LIDSTATEN ALS GEZAMENLIJKE VERWERKINGSVERANTWOORDELIJKEN VOOR DE FEDERATIEVE GATEWAY VOOR GRENSOVERSCHRIJDENDE VERWERKING TUSSEN NATIONALE MOBIELE APPLICATIES VOOR HET TRACEREN EN WAARSCHUWEN VAN CONTACTEN

AFDELING 1

Onderafdeling 1

Verdeling van verantwoordelijkheden

1) De gezamenlijke verwerkingsverantwoordelijken verwerken persoonsgegevens via de federatieve gateway overeenkomstig de door het e-gezondheidsnetwerk vastgestelde technische specificaties ([1]).

2) Elke verwerkingsverantwoordelijke is verantwoordelijk voor de verwerking van persoonsgegevens in de federatieve gateway overeenkomstig de algemene verordening gegevensbescherming en Richtlijn 2002/58/EG.

3) Elke verwerkingsverantwoordelijke richt een contactpunt met een functionele mailbox in voor de communicatie tussen de gezamenlijke verwerkingsverantwoordelijken en tussen de gezamenlijke verwerkingsverantwoordelijken en de verwerker.

4) Een overeenkomstig artikel 5, lid 4, door het e-gezondheidsnetwerk opgerichte tijdelijke subgroep wordt belast met het onderzoeken van kwesties die zich met betrekking tot de interoperabiliteit van nationale mobiele applicaties voor het traceren en waarschuwen van contacten en tot de gezamenlijke verantwoordelijkheid voor de daarmee samenhangende verwerking van persoonsgegevens aandienen, en met het faciliteren van de opstelling van gecoördineerde instructies aan de Commissie als verwerker. Onder andere kunnen de verwerkingsverantwoordelijken, in het kader van de tijdelijke subgroep, werken aan een gemeenschappelijke aanpak van de bewaring van gegevens op hun nationale backendservers, rekening houdend met de bewaartermijn die in de federatieve gateway is vastgelegd.

5) Instructies aan de verwerker worden door een van de contactpunten van de gezamenlijke verwerkingsverantwoordelijken toegezonden, in overeenstemming met de andere gezamenlijke verwerkingsverantwoordelijken van de bovengenoemde subgroep.

6) Alleen de daartoe door de aangewezen nationale autoriteiten of officiële instanties gemachtigde personen hebben toegang tot de persoonsgegevens van gebruikers die in de federatieve gateway worden uitgewisseld.

7) Elke aangewezen nationale autoriteit of officiële instantie houdt op een gezamenlijke verwerkingsverantwoordelijke te zijn met ingang van de datum waarop haar deelname aan de federatieve gateway wordt ingetrokken. Zij blijft echter verantwoordelijk voor de voorafgaand aan de terugtrekking verrichte verwerking in de federatieve gateway.

Onderafdeling 2

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

1) Overeenkomstig de artikelen 13 en 14 van de algemene verordening gegevensbescherming verstrekt elke verwerkingsverantwoordelijke de gebruikers van zijn nationale mobiele applicaties voor het traceren en waarschuwen van contacten ("de betrokkenen") informatie over de verwerking van hun persoonsgegevens in de federatieve gateway met het oog op de grensoverschrijdende interoperabiliteit van de nationale mobiele applicaties voor het traceren en waarschuwen van contacten.

2) Elke verwerkingsverantwoordelijke treedt op als contactpunt voor de gebruikers van zijn nationale mobiele applicaties voor het traceren en waarschuwen van contacten en behandelt de verzoeken tot uitoefening van de rechten van betrokkenen overeenkomstig de algemene verordening gegevensbescherming, zoals die door die gebruikers of hun vertegenwoordigers worden ingediend. Elke verwerkingsverantwoordelijke wijst een specifiek contactpunt aan voor de verzoeken van betrokkenen. Indien een gezamenlijke verwerkingsverantwoordelijke een verzoek van een betrokkene ontvangt dat niet onder zijn verantwoordelijkheid valt, stuurt hij het onverwijld door aan de desbetreffende gezamenlijke verwerkingsverantwoordelijke. De gezamenlijke verwerkingsverantwoordelijken verlenen elkaar op verzoek bijstand bij het behandelen van de verzoeken van de betrokkenen en beantwoorden elkaar onverwijld, en uiterlijk binnen 15 dagen na ontvangst van een verzoek om bijstand.

([1]) Met name de interoperabiliteitsspecificaties voor grensoverschrijdende doorgifteketens tussen goedgekeurde apps van 16 juni 2020, beschikbaar op: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0

3) Elke 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 federatieve gateway.

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 federatieve gateway worden verwerkt;

b) alle beveiligingsincidenten die verband houden met de verwerking in de federatieve gateway;

c) 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;

d) alle inbreuken op de technische en/of organisatorische waarborgen van de verwerking in de federatieve gateway.

3) De gezamenlijke verwerkingsverantwoordelijken melden, overeenkomstig de artikelen 33 en 34 van Verordening (EU) 2016/679 of na kennisgeving door de Commissie, alle inbreuken in verband met de verwerking in de federatieve gateway aan de Commissie, aan de bevoegde toezichthoudende autoriteiten en, in voorkomend geval, aan de betrokkenen.

AFDELING 3

Gegevensbeschermingseffectbeoordeling

Indien een verwerkingsverantwoordelijke, om te voldoen aan zijn verplichtingen uit hoofde van de artikelen 35 en 36 van de algemene verordening gegevensbescherming, informatie van een andere verwerkingsverantwoordelijke nodig heeft, zendt hij een specifiek verzoek naar de in afdeling 1, onderafdeling 1, punt 3, bedoelde functionele mailbox. De laatstgenoemde zal alles in het werk stellen om deze informatie te verstrekken.

BIJLAGE III

VERANTWOORDELIJKHEDEN VAN DE COMMISSIE ALS VERWERKER VOOR DE FEDERATIEVE GATEWAY VOOR GRENSOVERSCHRIJDENDE VERWERKING TUSSEN NATIONALE MOBIELE APPLICATIES VOOR HET TRACEREN EN WAARSCHUWEN VAN CONTACTEN

De Commissie:

1) zet een beveiligde en betrouwbare communicatie-infrastructuur op die de nationale mobiele applicaties van de aan de federatieve gateway deelnemende lidstaten voor het traceren en waarschuwen van contacten onderling verbindt, en waarborgt deze. Om aan haar verplichtingen als gegevensverwerker voor de federatieve gateway te voldoen, kan de Commissie een beroep doen op derden als subverwerkers. De Commissie stelt de gezamenlijke verwerkingsverantwoordelijken op de hoogte van voorgenomen wijzigingen met betrekking tot de toevoeging of vervanging van andere subverwerkers, zodat de verwerkingsverantwoordelijken in de gelegenheid worden gesteld om gezamenlijk bezwaar te maken tegen dergelijke wijzigingen, zoals vastgesteld in bijlage II, afdeling 1, onderafdeling 1, punt 4. De Commissie zorgt ervoor dat dezelfde verplichtingen inzake gegevensbescherming als uiteengezet in dit besluit van toepassing zijn op deze subverwerkers;

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

3) verwerkt de gegevens als volgt:

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

b) ontvangst van de in artikel 7 bis, lid 3, van dit uitvoeringsbesluit bedoelde gegevens die door nationale achtergrondservers zijn geüpload door te voorzien in een applicatieprogramma-interface (API) die nationale backendservers in staat stelt de relevante gegevens te uploaden;

c) opslag van de gegevens in de federatieve gateway zodra deze van de nationale backendservers zijn ontvangen;

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

e) wissen van de gegevens wanneer alle deelnemende backendservers ze hebben gedownload of 14 dagen na ontvangst, indien dat eerder is;

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

De verwerker treft de nodige maatregelen om de integriteit van de verwerkte gegevens te bewaren;

4) neemt alle geavanceerde organisatorische, fysieke en logische beveiligingsmaatregelen om de federatieve gateway in stand te houden. Hiertoe zal de Commissie:

a) een verantwoordelijke entiteit aanwijzen voor de federatieve gateway, de 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 federatieve gateway op zich nemen;

c) ervoor zorgen dat alle personen aan wie toegang tot de federatieve gateway 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 federatieve gateway. Deze procedures omvatten:

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. het mogelijk te maken, 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 beveiligingsmaatregelen, onder voorwaarden die in overeenstemming zijn met Protocol (nr. 7) bij het VWEU betreffende de voorrechten en immuniteiten van de Europese Unie ([2]);

([2]) Protocol (nr. 7) betreffende de voorrechten en immuniteiten van de Europese Unie (PB C 326 van 26.10.2012, blz. 266).

c) wijziging van de beheersprocedure om de gevolgen van een wijziging vóór de uitvoering ervan te documenteren en te meten, en de 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 verwerkingsverantwoordelijken en de Europese Toezichthouder voor gegevensbescherming onverwijld in kennis te stellen 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 federatieve gateway 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 een register van bezoekers bijhouden met het oog op de traceerbaarheid;

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 federatieve gateway controleren;

f) ervoor zorgen dat personen die toegang hebben tot de federatieve gateway geïdentificeerd en geauthenticeerd worden;

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

h) de integriteit van de via de federatieve gateway doorgegeven informatie bewaren;

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

j) waar nodig, maatregelen ten uitvoer leggen om ongeoorloofde toegang tot de federatieve gatewayvanaf 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 federatieve gateway, produceert regelmatig statistieken en registreert gegevens;

10) ondersteunt alle diensten van de federatieve gateway 24 uur per dag, 7 dagen per week in het Engels via telefoon, mail of webportal en accepteert oproepen van geautoriseerde oproepers: de coördinatoren van de federatieve gateway en hun respectieve helpdesks, projectmedewerkers en aangewezen personen van de Commissie;

11) staat, voor zover mogelijk, de 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 verwerkingsverantwoordelijken door informatie te verstrekken over de federatieve gateway, teneinde de verplichtingen uit hoofde van de artikelen 32, 35 en 36 van de algemene verordening gegevensbescherming na te komen;

13) zorgt ervoor dat de gegevens die binnen de federatieve gateway worden verwerkt, onbegrijpelijk zijn voor onbevoegden;

14) neemt alle nodige maatregelen om te voorkomen dat de gebruikers van de federatieve gateway ongeoorloofd toegang hebben tot doorgegeven gegevens;

15) neemt maatregelen om de interoperabiliteit en de communicatie tussen de verwerkingsverantwoordelijken voor de federatieve gateway 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 verwerkingsverantwoordelijken zijn verricht.”.