Nota van toelichting

1. Inleiding

Op 10 oktober 2020 is de Tijdelijke wet notificatieapplicatie covid-19 in werking getreden.[1] Deze tijdelijke wet expliciteert in de Wet publieke gezondheid (hierna: Wpg) dat de inzet van een notificatieapplicatie (hierna: CoronaMelder) onderdeel uitmaakt van de wettelijke taak tot bron- en contactopsporing door de GGD en van de taken van de minister van VWS tot de bevordering van de kwaliteit en doelmatigheid van de publieke gezondheidszorg, het zorgdragen voor de landelijke ondersteuningsstructuur en het geven van leiding aan infectieziektenbestrijding.
Met CoronaMelder kan vroegtijdig zicht worden verkregen op een mogelijke infectie met SARS-CoV-2 (hierna: het virus)[2] door bij te houden welke gebruikers in elkaars nabijheid zijn geweest en hen in voorkomende gevallen te waarschuwen over een mogelijke infectie met het virus.

Bij amendement van het lid van den Berg c.s.[3] is in het negende lid van artikel 6d Wpg geregeld dat de in het kader van CoronaMelder verwerkte gegevens kunnen worden uitgewisseld met andere lidstaten van de Europese Unie die een vergelijkbare notificatieapplicatie gebruiken indien deze uitwisseling bijdraagt aan het doel vroegtijdig zicht te kunnen verkrijgen op een mogelijke infectie met het virus door bij te houden welke gebruikers in elkaars nabijheid zijn geweest en hen in voorkomende gevallen te waarschuwen over een mogelijke infectie met het virus. Hiermee is een wettelijke grondslag gecreëerd voor de uitwisseling van gegevens via de European Union Federated Gateway Service (hierna: federatieve gateway). In paragraaf 2 van deze nota zal de werking van deze federatieve gateway verder worden toegelicht.

Daarnaast voorzag het amendement van den Berg c.s. in het tiende lid van artikel 6d Wpg dat voorschrijft dat bij algemene maatregel van bestuur in ieder geval de verwerkingsverantwoordelijke wordt aangewezen voor de gegevensverwerking die met toepassing van het negende lid plaatsvindt. Met het voorliggende besluit wordt hieraan invulling gegeven. In paragraaf 3 en in de artikelsgewijze toelichting wordt dit nader toegelicht.

Hoewel de strekking van dit besluit is beperkt tot het aanwijzen van de verwerkingsverantwoordelijke(n) voor de uitwisseling van gegevens met andere lidstaten van de Europese Unie wordt voor de duidelijkheid in deze nota van toelichting ook ingegaan op de wijze waarop deze uitwisseling plaatsvindt en welke waarborgen daarbij zijn getroffen.

2. Interoperabiliteit

Zoals in de toelichting op bovengenoemd amendement is opgemerkt kan interoperabiliteit een belangrijke bijdrage leveren aan het breder en sneller waarschuwen van mogelijk besmette mensen, in de grensregio's maar bijvoorbeeld ook voor vakantieverkeer.

Ook in Europees verband wordt onderkend dat de interoperabiliteit van notificatiesapplicaties kan bijdragen aan de bestrijding van het virus. Daarom zijn in het eHealth-netwerk afspraken gemaakt die de uitwisseling van gegevens tussen de in de verschillende lidstaten gebruikte notificatieapplicaties vergemakkelijken. Dat heeft geleid tot de federatieve gateway; een digitale infrastructuur die bestaat uit een

[1] Stb. 2020, 374.
[2] SARS-CoV-2 (severe acute respiratory syndrome coronavirus) is het virus dat de ziekte covid-19 kan veroorzaken.
[3] Kamerstukken II, 2019/20 35 538, nr. 12.

gemeenschappelijke interface waar aangewezen nationale autoriteiten of officiële instanties van lidstaten gegevens uit de aldaar gebruikte notificatieapplicaties kunnen uitwisselen. De technische specificaties van deze federatieve gateway zijn vastgelegd in richtsnoeren inzake interoperabiliteit[4] en het Uitvoeringsbesluit betreffende 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 (hierna: het Uitvoeringsbesluit).[5] Belangrijke uitgangspunten bij deze afspraken zijn:
- gebruikers hebben slechts één notificatieapplicatie nodig, waar ze zich ook bevinden in de Europese Unie;
- de gebruikte applicaties moeten daarom interoperabel zijn,
- de privacy en de gegevens van de gebruikers moeten veilig zijn,
- gebruikers kunnen de notificatieapplicatie elk moment de-installeren en
- de lidstaten deactiveren de notificatieapplicaties na de pandemie.

Er wordt in 22 landen gebruikt gemaakt van een notificatieapplicatie die in principe geschikt is voor aansluiting op de federatieve gateway. Op het moment van schrijven van deze nota van toelichting zijn Duitsland, Italië, Ierland, Spanje, Letland, Kroatië en Denemarken reeds op de federatieve gateway aangesloten. Het voornemen is dat Portugal, Polen, België, Cyprus, Finland, Litouwen en Slovenië in november 2020 aansluiten. Daarna is er weer een mogelijkheid tot aansluiting in januari 2021.

De uitwisseling van gegevens via de federatieve gateway verloopt als volgt.
De notificatieapplicaties van de deelnemende lidstaten wisselen, als ze in elkaars nabijheid zijn, onderling gepseudonimiseerde codes uit door middel van de zogenaamde exposure notification framework / application programming interface (api).[6]
De deelnemende lidstaten verstrekken vervolgens via de nationale backend server de gepseudonimiseerde codes van met het virus besmette gebruikers aan de federatieve gateway. Daarnaast ontvangen zij vanuit de federatieve gateway de gepseudonimiseerde codes van besmette gebruikers van alle andere deelnemende lidstaten. De lidstaten filteren deze gepseudonimiseerde codes en plaatsen ze vervolgens op de nationale backend server waar ze worden opgehaald door de in dat land gebruikte notificatieapplicatie. Vervolgens vindt zoals gebruikelijk lokaal op de smartphone een vergelijking plaats van de besmette codes en de op de smartphone opgeslagen codes. Als er sprake is van een match volgt een risicoweging en indien nodig een notificatie. De federatieve gateway brengt geen verandering in de werkwijze tussen de nationale server en de notificatieapplicatie.

Lidstaten kunnen ervoor kiezen om de gepseudonimiseerde codes op verschillende manieren te filteren. Zo kunnen zij ervoor kiezen om alleen de gepseudonimiseerde codes van gebruikers uit andere landen op de nationale backend server te zetten als deze gebruikers hebben aangegeven dat zij in de betreffende lidstaat zijn geweest. Ook zijn er lidstaten die in hun notificatieapplicatie willen inbouwen dat gebruikers ervoor kunnen kiezen dat de door hun gebruikte notificatieapplicatie alleen de besmette codes van bepaalde landen ophaalt. Voor deze filteropties is het nodig dat de via de federatieve gateway uitgewisselde gepseudonimiseerde codes zijn voorzien van een "land van

[4]Https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.
[5] Uitvoeringsbesluit 2020/1023 van de Europese Commissie (Pb. EU 2020, L 227 I) 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.
[6] Voor een meer uitgebreide beschrijving van deze werkwijze wordt verwezen naar paragraaf 3.1 van de memorie van toelichting op de Tijdelijke wet notificatieapplicatie covid-19, Kamerstukken II 2019/20, 35 538, nr. 3.

oorsprong" en eventueel van specifieke "landen van interesse". De federatieve gateway past zelf overigens geen filtering toe.

Het "land van oorsprong" zal door alle lidstaten aan de codes die zij via de federatieve gateway verstrekken worden toegevoegd. Enerzijds om de eerder genoemde filtering op specifieke landen mogelijk te maken en anderzijds zodat landen hun eigen codes eruit kunnen filteren. De deelnemende lidstaten ontvangen namelijk ook de eigen gepseudonimiseerde contactcodes van de gateway. De nationale backend server moet deze er weer uitfilteren voordat de overige via de federatieve gateway ontvangen gepseudonimiseerde contactcodes op de nationale backend server worden geplaatst.

Voor de optie waarbij wordt gewerkt met specifieke "landen van interesse" is het nodig dat duidelijk is in welk land gebruikers zijn geweest. Dat kan bijvoorbeeld door gebruikers in de notificatieapplicatie zelf specifieke landen van interesse aan te laten geven of door (de equivalent van) de GGD dat aan besmette gebruikers te laten vragen. Landen die niet specifieke "landen van interesse" willen opnemen in de gepseudonimiseerde codes volstaan met het toevoegen van de landcodes van alle deelnemende landen.

In Nederland zal geen gebruik worden gemaakt van de optie om te werken met specifieke "landen van interesse" omdat het vanuit privacyoogpunt niet wenselijk wordt geacht dat gebruikers moeten doorgeven in welk land zij zijn geweest. Eén van de uitgangspunten van CoronaMelder is immers dat geen locatiegegevens worden bijgehouden en dat in het kader van de app zo min mogelijk gegevens over de gebruiker worden verwerkt. Daarom zal bijvoorbeeld niet in CoronaMelder de mogelijkheid worden ingebouwd om alleen de gepseudonimiseerde codes van specifieke landen op te halen.

Daarnaast geldt overigens ook dat het feit dat een gebruiker niet in het buitenland is geweest niet per definitie betekent dat deze gebruiker niet in de nabijheid is geweest van een gebruiker van een notificatieapp van één van de deelnemende lidstaten. Hij kan immers ook in Nederland in de nabijheid van een buitenlandse appgebruiker zijn geweest, ook zonder dat hij daarvan op de hoogte was, bijvoorbeeld in het openbaar vervoer, in de bioscoop of in een supermarkt. Wel wordt nog onderzocht of het op termijn wenselijk is om CoronaMelder gebruikers in de app de mogelijkheid te geven om het ontvangen van codes uit het buitenland (zonder dat daarbij wordt gespecificeerd naar land) uit te zetten, bijvoorbeeld als blijkt dat de Europese uitwisseling leidt tot een substantiële verhoging van mobiel dataverkeer (met bijbehorende kosten).

3. Verwerking van persoonsgegevens

De European Data Protection Board (hierna: EDPB) heeft op 16 juni 2020 een verklaring opgesteld over de gevolgen van de interoperabiliteit van contactonderzoeksapps voor de gegevensbescherming.[7] De EDPB merkt daarin op dat "*de interoperabiliteit van applicaties voor contactonderzoek de doeltreffendheid van reeds bestaande maatregelen kan verhogen aangezien, ongeacht de gebruikte app, meer contacten kunnen worden getraceerd en meer meldingen kunnen worden gestuurd. Ook wijst de EDPB erop dat "Hierdoor het gebruik ervan wordt worden vereenvoudigd, met name voor personen in grensregio's, personen die reizen en personen die in hun beroep of op hun werkplek in contact komen met grote aantallen personen uit andere lidstaten (bijvoorbeeld in de toeristische sector)."* Uiteraard wijst de EDPB daarbij ook op mogelijke risico's rond gegevensbescherming. Zoals hieronder zal worden toegelicht worden deze risico's zoveel mogelijk afgedekt, onder meer door het treffen van beveiligingsmaatregelen en door niet meer gegevens te verwerken dan noodzakelijk. Lidstaten kunnen overigens alleen aansluiten bij de federatieve gateway als zij over een notificatieapplicatie beschikken die

[7]Https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_nl.pdf.

gebruik maakt van de api. Daarmee wordt tegemoet gekomen aan de door de EDPB gesignaleerde risico's voor interoperabiliteit van applicaties die geen gemeenschappelijk kader dan wel dezelfde technologische basis hebben.

Grondslag
Het verstrekken aan en ontvangen van gegevens uit de federatieve gateway is gerechtvaardigd op grond van artikel 6, eerste lid, aanhef en onder e, jo. artikel 9, tweede lid, aanhef en onder i, Algemene verordening gegevensbescherming (hierna: AVG) jo. artikel 3, eerste lid en 6d, eerste lid en negende lid van de Wpg. Het negende lid van artikel 6d Wpg sluit aan bij de aanbeveling van de EDPB om de nationale wetgeving ten aanzien van het gebruik van een notificatieapplicatie aan te passen als ervoor wordt gekozen om de betreffende gegevens uit te wisselen met andere lidstaten.

Beveiliging
Er is op Europees niveau een data protection impact assessment (hierna: DPIA) uitgevoerd op de verwerking van gegevens in de federatieve gateway. In deze DPIA zijn geen hoge risico's naar voren gekomen die niet kunnen worden afgedekt.

Daarnaast wordt op nationaal niveau een DPIA uitgevoerd op het door de Minister van VWS via de gateway verstrekken en ontvangen van gegevens. De functionaris gegevensbescherming heeft positief geadviseerd op het concept van deze DPIA. Het spreekt voor zich dat er niet wordt gestart met uitwisseling via de federatieve gateway voordat deze nationale DPIA is afgerond en de daarbij eventueel gebleken risico's zijn afgedekt.

In het eerder genoemde Uitvoeringsbesluit is onder meer opgenomen dat de federatieve gateway moet bestaan uit een beveiligde infrastructuur. Daarbij is ook geëxpliciteerd dat de Europese Commissie bij de verwerking van persoonsgegevens in het kader van de federatieve gateway gebonden is aan het besluit Euratom over de beveiliging van communicatie- en informatiesystemen binnen de Europese Commissie waarin de randvoorwaarden voor effectieve ICT-beveiliging zijn opgenomen.[8] Er zijn dan ook verschillende beveiligingsmaatregelen getroffen om de vertrouwelijkheid en integriteit van de via de federatieve gateway uit te wisselen gegevens te beschermen. Zo worden de aan de gateway verstrekte codes door elk land digitaal getekend en is het verkeer dat van en naar de federatieve gateway versleuteld.[9] Ook verifiëren de federatieve gateway en de nationale backend servers elkaars authenticiteit aan de hand van client-, signing-, en servercertificaten die via een door de deelnemende lidstaten vastgestelde procedure worden uitgewisseld. Verder zijn technische maatregelen genomen om te voorkomen dat anderen toegang kunnen krijgen tot de nationale backend servers en de federatieve gateway. Er zijn bijvoorbeeld externe audits uitgevoerd om de veiligheid van de werking van het systeem te borgen.

Tot slot is er voorzien in een strikt aansluitproces waarbij lidstaten die willen aansluiten op de federatieve gateway vooraf worden beoordeeld op geïmplementeerde technische en beveiligingsmaatregelen.

---

[8] Besluit (EU, Euratom) 2017/46 van de Commissie van 10 januari 2017 over de beveiliging van communicatie- en informatiesystemen binnen de Europese Commissie.
[9]Https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_certificate_governance_en.pdf.

Bewaartermijnen
De gepseudonimiseerde codes zijn gedurende zeven dagen op de federatieve gateway beschikbaar om door de deelnemende lidstaten te worden gedownload en worden daarna nog zeven dagen bewaard in de back-up systemen. Na veertien dagen worden de codes definitief verwijderd.

Verwerkingsverantwoordelijke
De Minister van VWS is de verwerkingsverantwoordelijke voor de verstrekking van gegevens aan de federatieve gateway en het ontvangen van de gegevens afkomstig van de federatieve gateway.

Voor de verwerking van gegevens in de federatieve gateway geldt dat de deelnemende lidstaten die persoonsgegevens verwerken in de federatieve gateway gezamenlijke verwerkingsverantwoordelijken zijn in de zin van artikel 26 van de AVG. De desbetreffende lidstaten wijzen daartoe nationale autoriteiten of officiële instanties aan. Voor Nederland is dat de minister van VWS.

Rechten van betrokkenen
Gebruikers van CoronaMelder worden ten minste drie dagen voor het aansluiten op de federatieve gateway via een bericht in de app hierover geïnformeerd. In dit bericht zal ook worden verwezen naar CoronaMelder.nl waar meer uitgebreide informatie over de federatieve gateway zal worden opgenomen.
Voor mensen die CoronaMelder downloaden nadat aansluiting op de federatieve gateway reeds heeft plaatsgevonden geldt dat zij tijdens het reguliere proces worden geïnformeerd over de werking van CoronaMelder, inclusief de interoperabiliteit. Daarbij worden zij verwezen naar de privacyverklaring waarin een en ander staat beschreven. Hiermee wordt aangesloten bij de eerdergenoemde verklaring van de EDPB waarin wordt benadrukt dat betrokkenen duidelijk dienen te worden geïnformeerd over de bijkomende verwerking die met interoperabiliteit gepaard gaat.

Zoals reeds toegelicht worden via de federatieve gateway slechts gepseudonimiseerde codes uitgewisseld. Deze codes zijn voor de (mede)verwerkingsverantwoordelijke niet te herleiden tot personen. Daarom zal over het algemeen sprake zijn van artikel 11 van de AVG waaruit volgt dat de artikelen 15 tot en met 20 van de AVG niet van toepassing zijn als de verwerkingsverantwoordelijke betrokkene niet (meer) kan identificeren. Ook de verklaring van de EDPB en het Uitvoeringsbesluit verwijzen overigens naar de toepasselijkheid van artikel 11 AVG.

4. Consultatie en advies
Het besluit is voor advies voorgelegd aan de Autoriteit Persoonsgegevens (hierna: AP). De AP merkt op dat de codes van alle gebruikers van CoronaMelder worden verstrekt aan de federatieve gateway en dat gebruikers op dat punt dus geen keuze hebben. De AP wijst erop dat dit de effectiviteit van een notificatieapplicatie ten goede komt, maar dat dit ook een schaalvergroting van de verwerking van de gepseudonimiseerde gezondheidsgegevens met zich meebrengt. De AP vraagt om deze keuze aan betrokkene te bieden dan wel toe te lichten waarom hier niet voor is gekozen.

De regering is de AP zeer erkentelijk voor de korte termijn waarbinnen de AP advies heeft uitgebracht. De regering meent, evenals de AP, dat vrijwilligheid bij het gebruik van CoronaMelder voorop moet staan. Dat is ook de reden dat in artikel 6d van de Wet publieke gezondheid is voorzien in een antimisbruikbepaling en er in verschillende fases van het gebruik van CoronaMelder toestemming van gebruikers wordt gevraagd. Daarbij worden gebruikers ook duidelijk geïnformeerd over welke verwerking er in het kader van CoronaMelder plaatsvindt. Zoals in paragraaf 3 is beschreven omvat die informatie ook het

delen van gepseudonimiseerde codes met de federatieve gateway. Het staat gebruikers vrij om naar aanleiding van deze informatie, dan wel op elk ander gewenst moment, te besluiten het gebruik van CoronaMelder te beëindigen.

Er is evenwel niet voor gekozen de optie in te bouwen dat kan worden gedifferentieerd naar het al dan niet óók verstrekken van gepseudonimiseerde (besmette) codes aan de federatieve gateway. Naar het oordeel van de regering doet het inbouwen van een dergelijke optie namelijk afbreuk aan een ander belangrijk uitgangspunt van CoronaMelder, namelijk het beginsel van dataminimalisatie.

Het bieden van de optie aan de gebruiker om gebruik te maken van de federatieve gateway zorgt voor een uitbreiding van de gegevensverwerkingen die in het kader van CoronaMelder plaatsvinden. Zo zal een besmette gebruiker die zijn gepseudonimiseerde codes wil delen met de server tevens via de GGD of via een nog in te bouwen optie in CoronaMelder moeten doorgeven of deze codes óók naar de federatieve gateway mogen. Op de server zal dus naar gelang de keuze voor interoperabiliteit onderscheid moeten worden gemaakt tussen de gepseudonimiseerde codes van de verschillende gebruikers. Dat wordt vanuit het eerder genoemde uitgangspunt van dataminimalisatie onwenselijk geacht. Daarbij is overigens ook van belang dat uit de keuze van gebruikers om al dan niet uit te wisselen met de federatieve gateway mogelijkerwijs kan worden afgeleid dat zij in het buitenland zijn geweest. Elk onderscheid dat gemaakt wordt tussen te verwerken gegevens heeft invloed op de herleidbaarheid van gegevens, hoe klein dat onderscheid ook mag zijn. Vanuit privacyoverwegingen is er daarom voor gekozen om zo min mogelijk onderscheidende gegevens mee te zenden met de codes.

Daarnaast acht de regering het van belang dat, zoals de AP ook opmerkt, interoperabiliteit de effectiviteit van CoronaMelder ten goede komt. Het virus stopt immers niet bij de grens en door het gebruik van de federatieve gateway wordt het bereik van CoronaMelder groter. Daarmee wordt in belangrijke mate bijgedragen aan het doel van CoronaMelder namelijk het bestrijden van de verspreiding van het virus door ketens van besmettingen zo veel en zo snel mogelijk te verbreken.

5. Artikelsgewijs

Artikel 1 bevat een aantal definities. Daarbij wordt voor de definitie van federatieve gateway verwezen naar artikel 1, eerste lid, onder j, van het Uitvoeringsbesluit waarin federatieve gateway wordt omschreven als "*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*".

In artikel 2 is geregeld dat de minister van VWS de verwerkingsverantwoordelijke is voor de verstrekking van gegevens aan de federatieve gateway en de verwerking van gegevens die via de federatieve gateway worden ontvangen.

Artikel 3 regelt dat de deelnemende lidstaten gezamenlijk verwerkingsverantwoordelijke zijn voor de verwerking van gegevens in de federatieve gateway en sluit daarmee aan bij het in het Uitvoeringsbesluit opgenomen artikel 7bis, vierde lid. De lidstaten wijzen daartoe een nationale autoriteit of officiële instantie aan. In artikel 7bis, vijfde lid, van het Uitvoeringsbesluit is geregeld dat de Europese Commissie daarbij optreedt als verwerker voor de deelnemende lidstaten.

Artikel 6d Wpg heeft een tijdelijk karakter en vervalt in beginsel op 10 januari 2021. Daarbij voorziet artikel II van de Tijdelijke wet notificatieapplicatie covid-19 in de mogelijkheid om deze wet bij koninklijk besluit eerder in trekken dan wel voor een periode van ten hoogste drie maanden te verlengen. Op het moment dat artikel 6d van de Wpg vervalt, vervalt ook de grondslag voor dit besluit. Voor de duidelijkheid is dit daarnaast ook expliciet opgenomen in artikel 4.

de Minister van Volksgezondheid,
Welzijn en Sport,