Ministerie van Volksgezondheid,
Welzijn en Sport

Deadline:

**Ontworpen door**

**Datum**

**Kenmerk**

**Zaaknummer**

# nota

(ter beslissing) Ontwikkeling en Bouw van *CoronaTester app*

---

Paraaf directeur

---

**Aanleiding**
Deze nota gaat in op beleidsmatige keuzes die samenhangen met de bouw van de *CoronaTester app*.

**Samenvatting**
1.Het uitgangspunt is dat er geen tot minimale verwerking van persoonsgegevens plaats moet vinden ten behoeve van gebruik van de CoronaTester app. Voor extra gegevensverwerking ontbreekt een duidelijke verwerkingsgrondslag waarmee ook de AP in zou kunnen stemmen. Discussies over de grondslag, dan wel het maken van wetgeving kost tijd. De AP zal zich hier intensief in mengen en een dergelijk traject proberen we te voorkomen.
2. Dat betekent dat er geen negatieve testresultaten uit spoor 2 opgeslagen zullen worden in een centrale database bij de GGD.
3. Dat betekent dat er geen testresultaten van private testaanbieders door de GGD worden verwerkt om testbewijzen af te geven. De grondslag om de negatieve testbewijzen te kunnen verstrekken aan de GGD is wankel. Dit kan alleen op basis van uitdrukkelijke toestemming en de AP zal die toestemming in deze context als onvoldoende vrij gegeven zien.
4. Omdat Spoor 2 niet gebruik zal maken van CoronIT, maar van een nieuw (NB nog te bouwen) ICT systeem, en CoronIT zich niet leent voor het maken van een testafspraak voor beide sporen, zal er op een andere manier tegemoet gekomen moeten worden aan de behoefte van een gemeenschappelijke ingang voor burger voor beide sporen.

**Beslispunten**

- Akkoord met een eerste gebruikersversie die alleen de functionaliteit Testbewijs heeft. Eventuele andere functionaliteiten worden later toegevoegd.

- Akkoord voor het inrichten van de functionaliteit Testbewijs waarbij de testresultaten niet centraal worden opgeslagen (optie a in deze nota).

Kenmerk

**Achtergrond**
Met de nota van 18 december zijn u 3 functionaliteiten gepresenteerd:

1. Toeleiding naar testlocatie,
2. Testbewijs en
3. Digitale ondersteuning Thuistesten

Het streven is om de eerste gebruikersversie gereed te hebben in de eerste week van februari. Deze eerste versie van de CoronaTester app biedt dan alleen nog de functionaliteit *Testbewijs.* De *Digitale ondersteuning Thuistesten* volgt op een later moment en de mogelijkheden voor de functionaliteit *Toeleiding* worden nog onderzocht. Het advies in de oplegnota is om in de eerste week van februari de inzet van testbewijzen van mogelijk te maken, zodat de inzet er van gestart kan worden, zodra dat wenselijk is.

**Status ontwikkeling van de *CoronaTester app*, per functionaliteit:**
De voorbereidingen van de app zijn in volle gang, waarbij de ontwikkelsnelheid mede af hangt van te maken beleidskeuzes in het juridische en privacy domein.

**1. Toeleiden naar testlocatie**
De partijen in spoor 2 hebben inmiddels besloten een eigen module te ontwikkelen om een test in te plannen, gekoppeld aan een betaal/afreken functionaliteit. Voor Spoor 1 bestaat al een planningsfunctionaliteit via Coronatest.nl. Tevens leent CoronIT zich technisch gezien niet voor het plannen van een afspraak. Hiermee vervalt de eerder aan u voorgelegde functionaliteit van het plannen van een testafspraak voor toegangstesten.
De behoefte aan een gemeenschappelijk digitale ingang/portaal "komt u voor Spoor 1 of 2" blijft echter wel bestaan en er wordt nu onderzocht hoe dit portaal er uit zou kunnen zien. Hierbij wordt gedacht aan bijvoorbeeld een stadskaart waarin alle teststraten van Spoor 1 (blauw bijv.) duidelijk zijn onderscheiden van de testlocaties van Spoor 2 (rood bijv.).

In de eerste gebruikersversie zal deze gemeenschappelijke functionaliteit nog niet opgeleverd zijn.
Overigens wordt er in overleg met de partijen in Spoor 2 een kader opgesteld voor de functionaliteit om een testafspraak in te plannen.

<u>Beslispunt 1:</u>
Gaat u ermee akkoord dat de eerste gebruikersversie alleen de functionaliteit Testbewijs heeft?

**2. Testbewijs**
Uitgangspunt is dat zowel testresultaten van Spoor 1 (GGD) als van teststraten uit Spoor 2 als basis kunnen dienen voor een testbewijs.

*Opslag van de testresultaten*
Bij de keuze voor centrale of decentrale opslag van de negatieve testresultaten om een testbewijs uit te kunnen genereren, is de kern, dat we op een

betrouwbare manier moeten weten of de persoon inderdaad een negatief testresultaat heeft gehad. Dat vergt:

- authenticatie van de persoon

- uitwisseling van testresultaat met de app

De authenticatie kan m.b.v. DigiD, als het een partij betreft\, die aan de aansluitvoorwaarden van Logius voldoet.

Voor de opslag en uitwisseling van het testresultaat zijn drie opties denkbaar, waarbij in de afweging het oorspronkelijke doel van de *CoronaTester App* goed voor ogen moet worden gehouden. Het doel is laagdrempelig testen en testbewijzen inzetten voor het openen van de samenleving. In de loop van de gesprekken over de app is daar weliswaar een doel bijgekomen, inzicht in de epidemiologische situatie, maar gelet op het korte tijdbestek waarin de app moet worden gerealiseerd en de verantwoordelijkheden van de betrokken partijen, is het de vraag of dit doel ook moet meewegen in het nemen van de beslissing.

Hierbij 3 opties verder uitgewerkt:

a) **Decentraal**: De gebruiker logt met zijn CoronaTester (CT) app in op de website van de testaanbieder en ontvangt het resultaat in zijn telefoon. Daar, decentraal, wordt er een bewijs van gegenereerd. Complexiteit: CT moet bij alle testaanbieders de testresultaten kunnen ophalen.

   Uitdrukkelijke toestemming voor doorbreken van het medisch beroepsgeheim is hier niet aan de orde, want testdata wordt niet verplaatst.

   De verwerkingsverantwoordelijkheid ligt bij de zorgaanbieder (=testleverancier), die de test heeft afgenomen, en daarmee het negatieve testresultaat levert. Dit zal als basis voor het testbewijs dienen.

   Het bouwen van deze optie duurt waarschijnlijk enkele weken. Om een testbewijs te kunnen genereren, moet de *CoronaTester app* 'gekoppeld' worden met de IT infrastructuur van alle testaanbieders / laboratoria. Elke zorgaanbieder zal het testresultaat in een door VWS te definiëren format aanleveren, zodat de *CoronaTester app* een testbewijs kan genereren. Cruciaal daarbij is de authenticatie, bij voorkeur middels DigiD of op een andere betrouwbare wijze.

   Alhoewel de oplevering van de eerste gebruikersversie dus vertraging kan opleveren, is het advies toch voor deze optie te kiezen. De optie is het meest AVG-proof omdat er geen testdata wordt opgeslagen of verplaatst. Er is dus geen toestemming van de AP of een wetswijziging nodig. Daarnaast worden met deze optie de verantwoordelijkheden van de GGD-en niet uitgebreid (met alle mogelijke vertraging vanwege het bespreken van een duidelijke governance). Ten slotte wordt door deze optie mogelijk het epidemiologisch inzicht beperkt.

b) **Centraal Publiek**: De gebruiker logt met zijn CT app in op de website van de GGD en ontvangt het resultaat in zijn telefoon. Alle private testaanbieders geven negatieve testresultaten door aan een nieuw aan te leggen database voor de GGD, maar alleen na toestemming van geteste persoon. Voordeel

voor CT is dat we maar één koppeling hoeven te maken en dat authenticatie met DigiD kan worden gedaan (nadeel: niet iedereen beschikt over DigiD). Uitdrukkelijke toestemming voor doorbreken van het medisch beroepsgeheim is nodig aan de arts van BV Toegangstesten voor het doorgeven van de negatieve testuitslagen aan database van de GGD, en dus aan een ander dan de geteste persoon zelf. AP neemt mogelijk niet genoegen met deze toestemming en eist mogelijk een wettelijke grondslag hiervoor.

Verwerkingsverantwoordelijkheid ligt bij de zorgaanbieder (GGD en BV Toegangstesten) die de test heeft afgenomen, en daarmee het negatieve testresultaat levert, dat als basis voor het testbewijs gaat dienen.

Het bouwen van deze optie duurt enkele weken. Juridisch zal hiervoor waarschijnlijk wetgeving voor nodig zijn. Voor de GGD is betreft een extra verwerking in een tweede database ten behoeve van een ander doel. De gegevens zijn verzameld voor het testen en melden van de uitslag aan betrokkene (GGD als zorgaanbieder) en niet voor het genereren van testbewijzen wat het doel is van de tweede database. Bovendien is de AP ten aanzien van uitdrukkelijke toestemming vrij strikt en zal zij de uitdrukkelijke toestemming voor het verstrekken van de private aanbieder naar de GGD niet als AVG proof zien. Daarnaast zullen de GGD hiermee ook verantwoordelijkheid naar zich toe trekken voor de uitslagen van andere aanbieders, omdat ze via haar database verstrekt worden. Deze optie kent dus verschillende juridische haken en ogen.

Het voordeel van deze optie is dat het epidemiologisch inzicht behouden wordt. Dit was overigens niet het primaire doel van de *CoronaTester- app.*

c) **Centraal Privaat**: De gebruiker logt met zijn CT app in op de website van het consortium spoor 2 en ontvangt het resultaat in zijn telefoon. Alle private testaanbieders (en eventueel ook de GGD) geven negatieve testresultaten door aan de consortium, maar alleen na toestemming van gebruiker. Voordeel voor CT is dat we maar één koppeling hoeven te maken. Nadeel: authenticatie met DigiD kan mogelijk niet gebruikt worden, juridische hordes en huidige situatie dat er nog geen ICT gereed is voor consortium.

Uitdrukkelijke toestemming voor doorbreken van het medisch beroepsgeheim is nodig voor de artsen van de zorgaanbieders van BV Toegangstesten voor het doorgeven van de negatieve testuitslagen aan de database. AP eist mogelijk een wettelijke grondslag hiervoor.

Verwerkingsverantwoordelijkheid ligt bij de zorgaanbieders van BV Toegangstesten, die de test hebben afgenomen, en daarmee het negatieve testresultaat leveren dat als basis voor het testbewijs gaat dienen.

Het bouwen van deze optie gaat waarschijnlijk enkele weken duren. Het vereist namelijk dat elke zorgaanbieder (=testleverancier) het testresultaat in eenzelfde, door VWS te definiëren format aanlevert aan de database, zodat de *CoronaTester app* het testresultaat kan lezen en er de juiste data uit kan distilleren. Bovendien zullen met de partijen in spoor 2 afspraken gemaakt te

worden over de bouw van de database. Tevens dient de te bouwen database een aansluiting op DigiD aan te vragen.

Van de drie opties bieden alleen optie b de Centraal Publieke optie, een goed inzicht in de epidemiologische situatie van het virus, en bestaat de mogelijkheid dat dit in optie a, de decentrale optie beperkt wordt en in optie c, de Centraal Private optie, gedeeltelijk beperkt zal worden. De decentrale optie (optie a) is het makkelijkst uitvoerbaar omdat er geen opslag gebouwd hoeft te worden en is daarmee ook het beste AVG-proof in te richten omdat er geen data worden verplaatst of centraal worden opgeslagen.

Het advies is dan ook de CoronaTester App verder uit te werken aan de hand van optie a: decentraal.

Beslispunt 2:
Gaat u akkoord met het niet centraal opslaan van de testresultaten (optie a)?

*Registratie van het testbewijs door organisator evenement*
Het uitgangspunt is dat we dit proces organiseren zonder extra verwerking van bijzondere persoonsgegevens. Dat geldt ook voor degene die toegang moet verlenen op basis van het testbewijs. Dit betekent dat er alleen sprake kan zijn van het tonen van het testbewijs.

Uit het advies van de Gezondheidsraad volgt dat de AVG van toepassing is indien het negatieve testbewijs bij de ingang wordt geregistreerd in een (elektronisch) systeem en raadpleegbaar is. En dat er een specifieke wettelijk grondslag nodig is voor de verwerking van de bijzondere persoonsgegevens. Omdat vooralsnog alleen behoefte lijkt aan controle zonder registratie, lijkt dit nu niet noodzakelijk. Hieruit volgen de volgende beleidsvragen:

- Hoe kan een fraude bestendig testbewijs worden ontwikkeld, dat snel en correct afgelezen kan worden, zonder dat het geregistreerd en raadpleegbaar is?
- Hoe wordt erop toegezien dat controlerende partijen hieraan voldoen?

Onder verantwoordelijkheid van VWS wordt een app ontwikkeld / aangeboden waarmee de gebruiker (bij voorkeur middels DigiD) inlogt op de database van een van de 3 bovengenoemde opties en daar inzage krijgt in zijn testresultaten. De gebruiker kan op basis daarvan *in de CoronaTester app* een testbewijs laten genereren. Dat testbewijs zal geen persoonsgegevens bevatten. Voldoende is dat gecontroleerd kan worden dat het bewijs geldig is en verstrekt is door een authentieke bron (in dit geval VWS). Dit wordt bewerkstelligd met cryptografie.

De mogelijkheid bestaat om in de app meerdere soorten testbewijzen voor verschillende doeleinden te genereren. Als voor bv internationaal reizen bepaalde persoonsgegevens wel vereist zijn (o.b.v. internationale afspraken), dan kan een testbewijs worden gegenereerd die die informatie wel bevat. Maar voor toegang tot bijv. een evenement is dat niet noodzakelijk en ook niet gewenst. Dit sluit goed aan bij het advies van de Gezondheidsraad dat bij iedere gelegenheid zal moeten worden afgewogen of een testbewijs de meest passende maatregel is.

Het testbewijs is beperkt geldig (bijv. 10 minuten), daarna wordt in de app een nieuw bewijs gegenereerd. Dit maakt overdracht/publicatie van/fraude met een verkregen bewijs van/aan een ander persoon veel moeilijker.

Voor de controle van het testbewijs worden de specificaties van het bewijs en de wijze van controle geopenbaard. Dit draagt bij aan het publiek vertrouwen in het testbewijs. Tevens geeft dit de mogelijkheid aan bijvoorbeeld evenementenorganisatoren om hun eigen ticketcontrole apparatuur te gebruiken (middels software aanpassing). Ook zal VWS zelf een controle app bouwen op basis van dezelfde specificaties en die beschikbaar stellen.

De controleur verkrijgt met het testbewijs geen toegang tot persoonsgegevens en verwerkt deze derhalve ook niet. Op deze wijze wordt ook voldaan aan het advies van de Gezondheidsraad.

Beslispunt 3:
Gaat u akkoord het testbewijs eenmalig te gebruiken en niet te registreren?

**3. Functionaliteit Digitale ondersteuning zelftesten**
Deze functie blijft gewenst en wordt ontwikkeld zodra er meer duidelijkheid is over de betrouwbaarheid van zelftesten en de beleidsmatige keuzes omtrent de vereiste begeleiding bij zelftesten.

**Privacy**
Net als bij CoronaMelder leggen we de lat voor deze functionaliteit wat betreft privacy en security heel hoog.

We werken aan een opzet van het testbewijs, waar de gebruiker zelf (met behulp van de app) zijn testresultaat ophaalt (met DigiD bij de GGD of bij een private testaanbieder). In de app zelf wordt het resultaat (cryptografisch) omgezet in een bewijs. Op deze wijze wordt er geen nieuwe verwerking van bijzondere persoonsgegevens uitgevoerd. Het testbewijs zelf kan in meerdere varianten worden vormgegeven. Default hebben we gekozen voor een variant waarin géén persoonsgegevens zijn opgenomen. De controleur van het bewijs ziet alleen of het bewijs geldig is of niet.

N.B. voor specifieke toepassingen (bijv. voor internationaal reizen waar vanuit regelgeving vereist is dat er wel bepaalde persoonsgegevens opgenomen moeten worden) kan een aangepaste versie van testbewijs worden gegenereerd. In de systeemarchitectuur zijn maatregelen genomen die overdracht van het bewijs tussen personen zinloos maken. Wie het bewijs mag controleren kunnen we nauwgezet reguleren doordat een specifieke cryptografische sleutel nodig is om het bewijs te valideren.

De systemen worden ontworpen op het beveiligingsniveau statelijke actoren, net als BRBA. Alle onderdelen worden onder open source licentie gepubliceerd.