Gegevensbeschermingseffectbeoordeling (PIA)

VWS | Directie Informatiebeleid / CIO

PIA CoronaCheck en Testbewijs

Den Haag, 26-04-2021 / Status: Vastgesteld

Vaststelling verwerkersverantwoordelijke:
Naam: , Directeur Programmadirectie Covid-19

Kennisgenomen van FG-advies
Acceptatie restrisico na genomen maatregelen: akkoord

Datum akkoord: 26 april 2021

Advies Functionaris voor Gegevensbescherming VWS: 19 april 2021

Gegevensbeschermingseffectbeoordeling (PIA)

VWS | Directie Informatiebeleid / CIO

PIA CoronaCheck en Testbewijs

Contact:

Ministerie van Volksgezondheid, Welzijn en Sport
Directie Informatiebeleid/CIO
Parnassusplein 5
2511 VX Den Haag

Versie: 1.2, 26 april 2021

Inhoud

Inleiding

Deze PIA is opgesteld door het programma 'Realisatie Digitale Ondersteuning' binnen het Ministerie Volksgezondheid, Welzijn en Sport (hierna VWS) en geldt voor het 'Testbewijs'. Het testbewijs is een middel voor een persoon om aan te geven dat deze persoon recent negatief is getest op Corona. In deze PIA wordt beschreven welke privacybeschermende maatregelen zijn genomen om het testbewijs als dergelijk middel in te kunnen zetten.

Deze PIA is ziet op de apps CoronaCheck en CoronaCheck Scanner en het genereren van een papieren testbewijs via coronacheck.nl voor pilot evenementen die vanaf 22 april 2021 worden gehouden. Tijdens deze pilots wordt gebruikgemaakt van een versie van de apps CoronaCheck en CoronaCheck Scanner, die voorafgaat aan de versie zoals deze is beschreven aan het wetsvoorstel en bijbehorende Memorie van Toelichting, versie 8 maart 2021 die ter consultatie is aangeboden[1].

[1] https://www.internetconsultatie.nl/wetsvoorsteltestbewijzen

A. Beschrijving kenmerken gegevensverwerking

1. Voorstel

Nederland wordt, net als de rest van de wereld, geconfronteerd met de uitbraak van het SARS-CoV-2, een virus dat kan leiden tot de ziekte COVID-19. De verspreiding van SARS-CoV-2 wordt beteugeld door diverse maatregelen. Daar waar bewegingsvrijheid wordt beperkt door een lockdown, ontstaat de behoefte om op een gecontroleerde manier de samenleving weer te openen. Het testbewijs is een middel wat daarbij kan ondersteunen.

Het testbewijs is een bewijs, met tijdelijke geldigheid, dat iemand negatief getest is op COVID-19. Dit bewijs kan worden gebruikt om toegang te geven tot specifieke activiteiten en voorzieningen. Het testbewijs maakt het (in combinatie met andere risico beperkende maatregelen) mogelijk om daar waar verlichting van de lockdown mogelijk is, dit ook te doen.

De organisatoren van activiteiten en voorzieningen waarvoor een testbewijs gevraagd wordt, dienen te controleren of de deelnemer een geldig testbewijs heeft en gebruiken daarvoor de applicatie CoronaCheck Scanner. Deelnemers aan de pilots en bezoekers van de voorzieningen moeten zich daarvoor laten testen en - samen met een legitimatiebewijs - het testbewijs tonen bij de betreffende activiteit of voorziening. Daarvoor kunnen zij de applicatie CoronaCheck gebruiken of een papieren testbewijs dat gegenereerd kan worden via de website coronacheck.nl. De applicaties CoronaCheck en CoronaCheck Scanner en de website coronacheck.nl zijn onder verantwoordelijkheid van de Minister van VWS ontwikkeld.

Dit document bevat een Privacy Impact Assessment, (hierna: PIA) van het gebruik van persoonsgegevens[2] voor het testbewijs, de beide applicaties en coronacheck.nl, conform artikel 35 van de Algemene Verordening Gegevensbescherming (hierna: AVG).[3]

Gebruikte afkortingen

AVG	Algemene Verordening Gegevensbescherming
Controleur	Iemand die de geldigheid van een testbewijs controleert
Persoon	De persoon die een testbewijs wil genereren (zowel digitaal als fysiek) om deel te nemen aan een pilot evenement of een pilot locatie wil bezoeken.
PIA	Privacy impact assessment
SON	Stichting Open Nederland
Testresultaat	Resultaat van een test dat door teststation wordt verstrekt aan persoon
Testbewijs	Deel van gegevens van testresultaat nodig is om bij toegang te tonen
Verstrekker	Teststation die een testresultaat verstrekt

[2] Uitgangspunt van deze PIA is het voorgenomen gebruik van (persoons)gegevens zoals bekend op 21 april 2021.
[3] Deze PIA ziet op de pilot versie van beide applicaties en het genereren van een fysiek testbewijs via coronacheck.nl.

VWS	Volksgezondheid, Welzijn en Sport
Wpg	Wet publieke gezondheid

2. Scope van de PIA

Een wetsvoorstel om testbewijzen op grote schaal in te kunnen gaan zetten bij het heropenen van de samenleving is ter consultatie[4] aangeboden. Deze consultatie is gesloten op 15 maart 2021. In dit voorstel wordt de Wet publieke gezondheid (Wpg) gewijzigd. Door preventief te testen en daarvan een testbewijs te verstrekken kunnen verschillende evenementen en activiteiten eerder veilig georganiseerd worden.

Het Ministerie van VWS is op zoek naar meerdere bouwstenen die bijdragen aan preventie en reductie van het risico van verspreiding van het COVID-19 virus. De ontwikkelde pilot evenementen en aangewezen deelnemende locaties zijn gericht op het vergaren van kennis en data rondom evenementen in tijden van COVID-19. Aan de hand van de onderzoeksresultaten wordt toegewerkt naar veilige en verantwoorde evenementen met een verhoogde bezoekerscapaciteit, zoals voorheen. VWS werkt hierbij samen met Stichting Open Nederland (SON) aan de uitbreiding van de testcapaciteit en met de organisatoren van pilotevenementen en –locaties. Hierbij geldt dat de testcapaciteit wordt ingericht door SON en dat de testen worden uitgevoerd door teststations. Bij het gebruik van CoronaCheck of een fysiek testbewijs in deze pilotfase wordt alleen gebruik gemaakt van de testcapaciteit zoals ingericht door SON.

Totdat de voorgestelde wetswijziging is goedgekeurd, bestaat de behoefte om in diverse pilots en proefevenementen gebruik te maken van CoronaCheck, het genereren van een papieren testbewijs via coronacheck.nl en CoronaCheck Scanner en ook op dit punt kennis en data te vergaren.

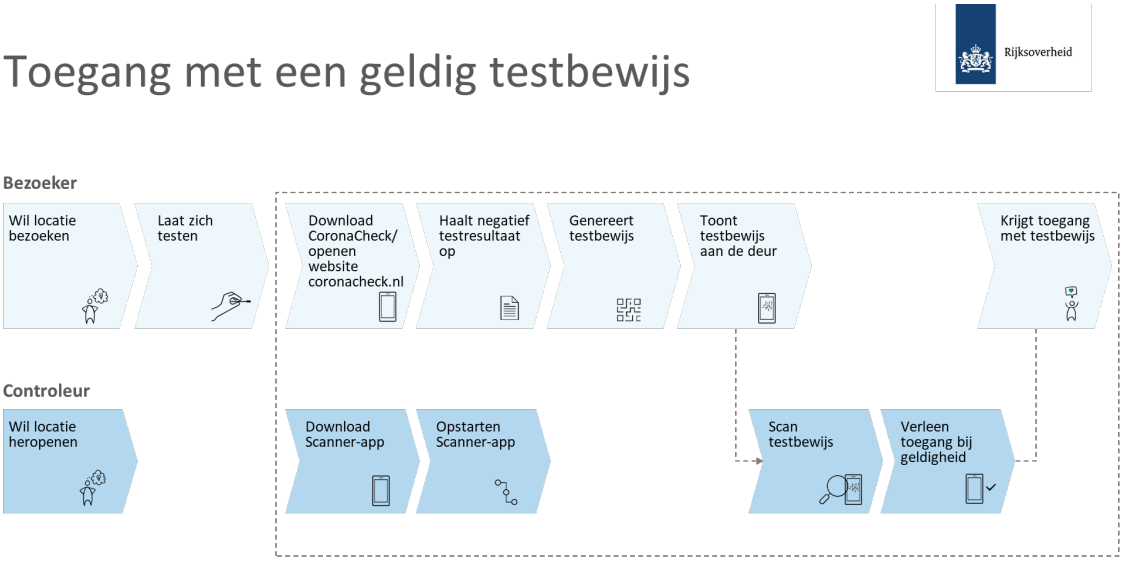
Binnen de scope van deze PIA valt:
- het ophalen van een negatief testresultaat bij een teststation (verstrekker);
- het genereren van een digitaal of fysiek testbewijs (in CoronaCheck of via de website coronacheck.nl);
- de validatie van het testbewijs voor toegang (door CoronaCheck Scanner).

Buiten de scope van deze PIA valt de gegevensverwerking bij de teststations zoals ingericht door of namens SON. Buiten de scope van deze PIA valt daarmee onder meer het maken van de testafspraak, het uitvoeren van de test, het informeren van de persoon over zijn testresultaat en het digitaal tekenen van het testresultaat door het teststation.

In de plaatjes en beschrijvingen hierna wordt het proces in zijn volledigheid inzichtelijk gemaakt en wordt specifiek aangegeven wat wel en niet in scope is van het gebruik van (persoons)gegevens.

Grafisch ziet de scope er als volgt uit, waarbij de stippellijn de scope van deze DPIA vormt.

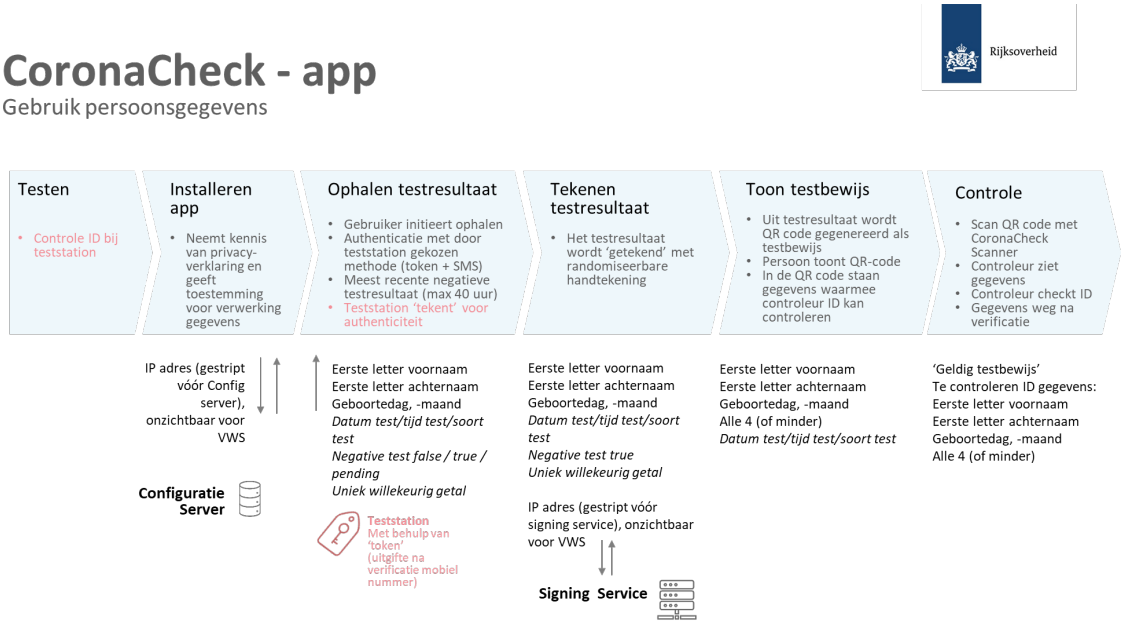
[4] https://www.internetconsultatie.nl/wetsvoorsteltestbewijzen.



CoronaCheck (app) is te downloaden in de Apple App Store of de Google Play Store. De gegevens die Apple en Google gebruiken voor toegang tot de Stores (zoals een emailadres) worden in het kader van CoronaCheck niet gebruikt. Als zodanig valt de verwerking daarvan door Apple en Google buiten de scope van deze PIA.

Er zijn twee routes die een persoon kan kiezen om een testbewijs te genereren. De eerste wijze is het gebruik van de app CoronaCheck, waarbij er een digitaal testbewijs wordt gegenereerd. De tweede wijze is het genereren van een fysiek testbewijs via de website coronacheck.nl. Voor de duidelijkheid worden beide routes in onderstaande alinea's apart en volledig beschreven. Het is bovendien mogelijk om van beide routes gebruik te maken, waarbij met dezelfde token zowel een fysiek als een digitaal testbewijs kan worden gegenereerd. Het omzetten van een testresultaat naar een testbewijs is wel gelimiteerd, hierbij geldt dat er met CoronaCheck maximaal twee keer met dezelfde token een testbewijs kan worden gegenereerd. Voor het genereren van een fysiek testbewijs geldt dat dit kan met dezelfde token zolang deze geldig is, waarbij misbruik preventie door de verstrekker (en valt daarmee buiten de scope van deze PIA) van toepassing is.

Beschrijving van het gebruiksproces (digitaal testbewijs)
Deze alinea beschrijft het proces waarbij gebruik wordt gemaakt van CoronaCheck voor het genereren van een digitaal testbewijs. De eerste stap is dat de persoon een corona test doet bij een testaanbieder (hierna ook 'verstrekker' genoemd). Dit kan een PCR test zijn, of een andere goedgekeurde test. Bij de afname van de test is de verstrekker verplicht de identiteit van de persoon te controleren, dit valt buiten de scope van de PIA en heeft daarom in onderstaand plaatje een afwijkende kleur.



Bij de verstrekker wordt het emailadres en mobiele nummer van de persoon gevraagd, dit is nodig om (op het moment dat het testresultaat beschikbaar is) het testresultaat met de persoon te kunnen delen. Het gebruik van deze persoonsgegevens valt daarmee buiten scope van deze PIA en is herkenbaar aan de afwijkende kleur in het plaatje.

De persoon installeert de CoronaCheck app op de smartphone[5] via de Apple Store of de Google Play Store. Na installatie van de app, zoekt de app contact met de Configuratie Server van VWS, om daar de meest recente instellingen en actueel sleutelmateriaal op te halen.

Zodra het testresultaat beschikbaar is ontvangt de persoon van de testaanbieder een email met daarin een token (een unieke code). Vervolgens vult de persoon via de smartphone in de CoronaCheck app deze token in. De persoon krijgt ter controle een SMS op het mobiele telefoonnummer dat is opgegeven bij het teststation om het ophalen van het testresultaat te bevestigen. De persoon haalt vervolgens via de CoronaCheck app op de smartphone de testresultaten op bij de testaanbieder en plaatst deze in de CoronaCheck app van de persoon.

De testaanbieder tekent het testresultaat cryptografisch, waarmee CoronaCheck kan controleren dat het testresultaat ook daadwerkelijk van de testaanbieder afkomstig is. De wijze van tekenen vindt plaats bij de testaanbieder en is daarmee buiten scope van deze PIA.

Op basis van het testresultaat dat de persoon in CoronaCheck heeft opgehaald laat de persoon het testresultaat in de CoronaCheck app tekenen door een signing service. Dit 'tekenen' houdt in dat CoronaCheck het testresultaat voorziet van een gerandomiseerde handtekening. Deze gerandomiseerde handtekening zorgt dat het testbewijs steeds op een verschillende manier is getekend. Zo kan geen van de betrokken partijen (testaanbieder VWS, controleur) volgen waar mensen dit testbewijs gebruiken. Ten slotte genereert CoronaCheck een testbewijs. Het testbewijs dat middels CoronaCheck wordt gegenereerd bestaat uit een QR-code en uit een set identificerende gegevens (eerste letter voornaam, eerste letter achternaam, geboortedag en

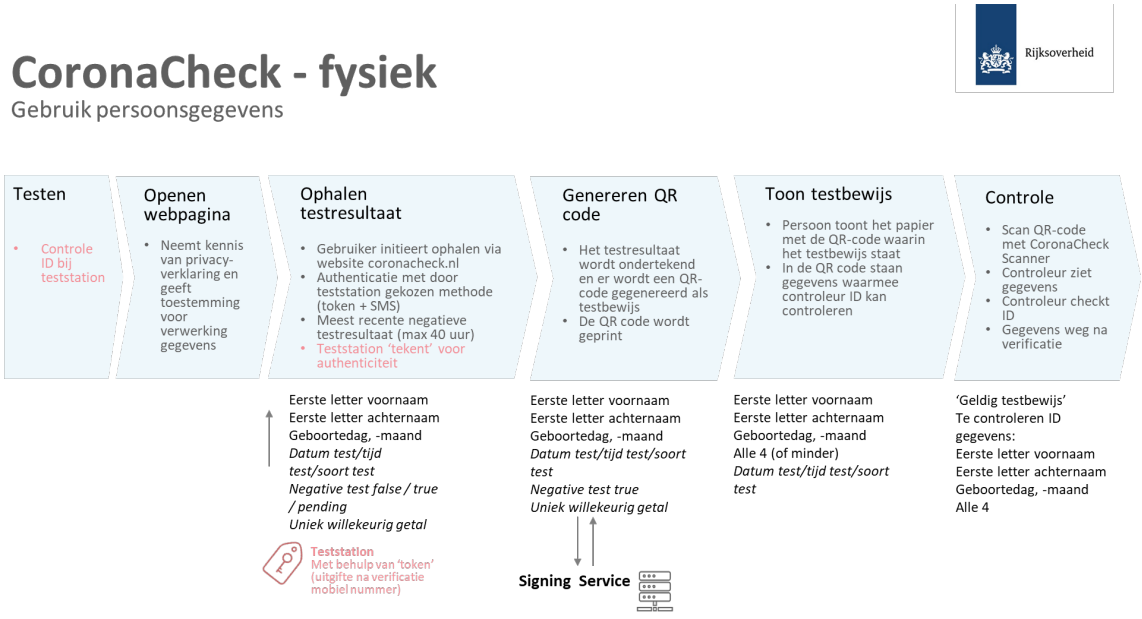
[5] Vanaf Android 6 en iOS11.

geboortemaand). Deze set identificerende gegevens is verwerkt in de QR-code en wordt separaat weergegeven als aparte regel onder de QR-code. De QR-code is 40 uur geldig.

In het licht van het beginsel van privacy by design wordt de set van identificerende gegevens automatisch verder beperkt (dit kan met één of meer van de vier typen identificerende gegevens) wanneer de set identificerende gegevens een te hoge herleidbaarheid van een persoon tot gevolg heeft. Dit is bijvoorbeeld het geval wanneer de eerste letter voornaam en eerste letter achternaam bestaan uit de letters 'X' en 'Y'. Dit geldt alleen voor het genereren van een digitaal testbewijs in CoronaCheck.

Beschrijving van het gebruiksproces (fysiek testbewijs)
Deze alinea beschrijft het proces waarbij gebruik wordt gemaakt van coronacheck.nl voor het genereren van een fysiek testbewijs. Een persoon kan ervoor kiezen om het testbewijs uit te printen. Daartoe is het nodig dat de persoon kan beschikken over een computer met printer. Dit kan ook een computer / printer zijn bij familie of buren.

De eerste stap is wederom dat de persoon een corona test doet bij een testaanbieder (hierna ook 'verstrekker' genoemd). Dit kan een PCR test zijn, of een andere goedgekeurde test. Bij de afname van de test is de verstrekker verplicht de identiteit van de persoon te controleren, dit valt buiten de scope van de PIA en heeft daarom in onderstaand plaatje een afwijkende kleur. Bij de verstrekker wordt het emailadres en mobiele nummer van de persoon gevraagd, dit is nodig om (op het moment dat het testresultaat beschikbaar is) het testresultaat met de persoon te kunnen delen. Het gebruik van deze persoonsgegevens valt daarmee buiten scope van deze PIA en is herkenbaar aan de afwijkende kleur in het plaatje.



Wanneer de persoon gebruik wil maken van een fysiek testbewijs kan de persoon naar de website coronacheck.nl gaan. Voordat het programma om een testbewijs te genereren in de browser van de persoon kan worden gedraaid dient de persoon eerst toestemming te geven voor de verwerking van zijn/haar persoonsgegevens. Indien de persoon toestemming geeft kan de persoon in het browserprogramma zijn/haar token invoeren waarna een bevestigingscode wordt verzonden via

SMS. Hierna wordt het testresultaat eerst getekend door de verstrekker en daarna door de signing service, zoals ook gebeurt met het testbewijs in CoronaCheck. Dit 'tekenen' houdt in dat het testresultaat is voorzien van een gerandomiseerde handtekening. Deze gerandomiseerde handtekening zorgt dat het testbewijs steeds op een verschillende manier is getekend. Zo kan geen van de betrokken partijen volgen waar mensen dit testbewijs gebruiken. Het testbewijs, in de vorm van een QR-code, dat door middel van coronacheck.nl wordt gegenereerd bestaat uit een testresultaat en uit een set identificerende gegevens (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand). Deze set identificerende gegevens is verwerkt in de QR-code en wordt separaat weergegeven als aparte regel onder de QR-code. De QR-code is 40 uur geldig. Daarna kan het testbewijs als worden geprint als fysiek testbewijs. Op de print met het fysieke testbewijs staat een vergelijkbare QR-code als op het digitale testbewijs.

Toegang met testbewijs
Voordat toegang kan worden verkregen wordt dan wel het fysieke dan wel het digitale het testbewijs gecontroleerd door een 'controleur'. De controleur maakt voor de controle op een geldig negatief testbewijs gebruik van de CoronaCheck Scanner app.

Deze CoronaCheck Scanner app heeft als functionaliteit het lezen van de QR-code en het op basis daarvan aangeven of deze persoon inderdaad beschikt over een geldig negatief testbewijs.

Componenten van CoronaCheck
CoronaCheck bestaat uit de volgende componenten:
- De CoronaCheck app – dit is de app die de persoon gebruikt om een testbewijs te genereren en vervolgens te presenteren.
- De CoronaCheck Scanner app – dit is de app die de controleur gebruikt om te controleren of iemand beschikt over een geldig negatief testbewijs.
- Een configuratie server en een Signing service.

Voor het beheer van beide apps is een configuratie server actief. Zo wordt bij het opstarten van de app de configuratie opgehaald. Deze configuratie server bevat instellingen zoals de duur van de geldigheid van testbewijzen en sleutels die gebruikt worden voor de beveiliging. Ook bevat de configuratie server een mogelijkheid waarmee, de service om testbewijzen te valideren éénmalig of volledig beëindigd kan worden. Dit is bijvoorbeeld nuttig als de inzet van de app definitief niet meer wenselijk wordt geacht.

Met de Signing service wordt ieder testresultaat in de CoronaCheck app cryptografisch 'getekend'. Het resultaat hiervan is een geldig testbewijs die in de app als QR-code wordt getoond.

3. Verwerkingen van persoonsgegevens

De volgende gegevens worden gebruikt.
- In het **testresultaat** zijn de volgende gegevens opgenomen:
    - Geregistreerde datum en tijdstip van testen (t.b.v. geldigheidsduur testresultaat), afgerond op een heel uur.
    - Type test (t.b.v. eventueel te maken onderscheid in verschillende testsoorten in de toekomst).
    - Indicatie negatieve test ('true'). Hierbij betekent 'true' dat er een negatieve test is overlegd en iemand dus tijdens de test niet besmet was. Een positief testresultaat wordt niet via een aparte procedure teruggekoppeld aan de geteste persoon en is volledig buiten scope van deze PIA.

  - Eerste letter van de voornaam en de eerste letter van de achternaam, aangevuld met de geboortedag en geboortemaand van getest persoon.
  - Digitale handtekening van Verstrekker (waarmee ze verantwoording dragen voor het juist uitgegeven negatieve testresultaat en waarmee kan worden gecontroleerd of de gegevens in het resultaat niet zijn aangepast nadat ze door de drager zijn ontvangen). De digitale handtekening bevat ook het exacte tijdstip dat die handtekening gezet is.

  Deze gegevens worden in de app op de smartphone van de persoon opgeslagen.

- In het **testbewijs** is opgenomen[6]:
  - Geregistreerde datum en tijdstip van testen (t.b.v. geldigheidsduur testresultaat), afgerond naar het eerstvolgende hele uur
  - Type test (t.b.v. eventueel te maken onderscheid in de toekomst)
  - Indicatie negatieve test (true)
  - Digitale handtekening van de Signing Service (waarmee kan worden gecontroleerd of de gegevens in het resultaat niet zijn aangepast nadat ze door de drager zijn ontvangen).
  - Eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand van de gebruiker.
  - Dit testbewijs wordt via de CoronaCheck app verwerkt en als QR-code op de smartphone van de persoon gepresenteerd en opgeslagen of in de browser van de persoon via coronacheck.nl getoond.

In het testresultaat en in het testbewijs is ook een uniek willekeurig getal (niet persoonsgebonden) opgenomen om dubbele uitgifte van bewijzen te kunnen voorkomen. Dit getal wordt als metadata gelezen door de signing service.

Het omzetten van een testresultaat in een testbewijs gaat via een configuratie service en de signing service van VWS. Het testresultaat wordt hiervoor naar de server van VWS gestuurd. Inherent aan internetcommunicatie is dat hiervoor een IP-adres wordt gebruikt. Het IP-adres van wordt binnen de beheeromgeving niet vastgelegd, deze wordt als het ware 'gestript'[7] voordat deze bij de signing service komt, zodat de signing service niet ziet welk testbewijs aan welk IP-adres is gekoppeld. VWS ziet dus geen externe IP-adressen, maar alleen het interne IP adres van de verwerker. Het strippen van het IP-adres gebeurt door Prolocation, dit is een verwerker van VWS. Het testresultaat zelf is versleuteld. Prolocation kan de gegevens in het testresultaat niet zien. Vervolgens wordt de digitale handtekening van de signing service gezet en wordt het testbewijs teruggestuurd naar de gebruiker. Dit testbewijs wordt in de app of op via het browserprogramma in coronacheck.nl getoond in de vorm van een QR-code.

- In de CoronaCheck Scanner app worden de volgende gegevens gepresenteerd:
  - Indicatie: 'Persoon beschikt over geldig negatief testbewijs' (groen scherm) / 'Persoon beschikt niet over geldig negatief testbewijs' (rood scherm).
  - Set identificerende gegevens (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand) aan de hand waarvan de controleur de identiteit van de gebruiker kan controleren met zijn/haar identiteitsbewijs.

[6] 'Opgenomen' betekent in dit geval dat deze gegevens worden gerepresenteerd in een (voor mensen niet leesbare) QR-code.

[7] Door een derde partij (Prolocation) worden deze (externe) IP-adressen vervangen door een intern IP-adres.

CoronaCheck Scanner legt van deze controles geen gegevens vast, de app beperkt zich tot het tonen van de genoemde indicatie ('geldig negatief testbewijs'). De gegevens die verdwijnen van het scherm bij de eerstvolgende scan of anders uiterlijk na 240 seconden (dit is configureerbaar).

4. Doeleinden van de beoogde gegevensverwerking

Het testbewijs is een nieuw middel in het openen van de samenleving uit een lockdown en kan samen met andere middelen worden ingezet (bijvoorbeeld afstand houden, dragen mondkapje). Een testbewijs laat zien dat iemand binnen de afgelopen periode negatief is getest. Doel einde van CoronaCheck is dat een persoon bij toegang tot een bepaalde faciliteit aan de poort op digitale wijze kan laten zien dat hij of zij beschikt over een negatief testbewijs dat niet ouder is dan vastgestelde termijn van 40 uur.

5. Betrokken partijen

Bij onderstaande toelichting van de betrokken partijen, wordt ingegaan op de verwerkingen die plaatsvinden binnen CoronaCheck en het genereren van een papieren testbewijs via coronacheck.nl. Andere verwerkingen die plaatsvinden door – bijvoorbeeld – de verstrekkers zijn buiten scope en worden derhalve niet toegelicht.

SON is een betrokken partij, omdat SON in de pilotperiode testaanbieders inzet. Testaanbieders die testresultaten aanleveren ('verstrekkers') zijn eveneens betrokken partijen. CoronaCheck of coronacheck.nl haalt op verzoek van de persoon bij verstrekkers die zijn aangesloten bij SON de negatieve testresultaten op. Verstrekkers zijn de partijen die testen uitvoeren. Voor het gebruik van persoonsgegevens die zij vragen voor het uitvoeren van testen en het verstrekken van testresultaten (denk aan emailadres en/of nummer van smartphone) zijn zij zelfstandig verwerkingsverantwoordelijk.

Op dit moment zijn de volgende partijen betrokken:

- Testcapaciteit die door SON wordt ingericht – deze Stichting zorgt (in nauwe samenwerking met EZK, OCW) voor een versnelde uitrol van testcapaciteit.[8]
- De organisatoren van pilotevenementen. Met deze organisaties worden geen (persoons)gegevens uitgewisseld.
- Prolocation als verwerker voor de verwerkingen die plaatsvinden op de signing service. Met Prolocation is een verwerkersovereenkomst gesloten.

De CoronaCheck app en de website coronacheck.nl zijn ontwikkeld door het ministerie van VWS. De minister van VWS is verantwoordelijk voor de regie op de wijze waarop we uit de lockdown komen en de wijze waarop CoronaCheck daarvoor wordt ingezet. De Minister is daarmee opdrachtgever voor de ontwikkeling van de CoronaCheck en de CoronaCheck Scanner app.

De minister van VWS is de verwerkingsverantwoordelijke voor de verwerkingen van persoonsgegevens die bij het genereren van een testbewijs via CoronaCheck en coronacheck.nl worden gebruikt. Binnen CoronaCheck Scanner worden geen persoonsgegevens vastgelegd. Deze verantwoordelijkheid geldt voor de CoronaCheck app, coronacheck.nl (ten aanzien van het genereren van een fysiek testbewijs) en de CoronaCheck Scanner app, de werking van de

[8] Zie ook https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z03637&did=2021D08036

configuratie server en de Signing service (de Minister van VWS schakelt hiervoor Prolocation als verwerker in). VWS stelt verder eisen aan de wijze waarop de testresultaten door de verstrekkers worden aangeleverd.

6. Ontvangers

CoronaCheck en coronacheck.nl tonen alleen gegevens aan de geteste persoon: de persoon ontvangt via e-mail het testresultaat van de verstrekker. Dit resultaat wordt op verzoek van de persoon door CoronaCheck of coronacheck.nl omgezet in een testbewijs.

De controleur scant met CoronaCheck Scanner de QR-code in CoronaCheck of de QR-code op het papieren testbewijs. De controleur krijgt daarbij te zien of de persoon beschikt over een geldig negatief testbewijs door middel van een groen of een rood scherm in CoronaCheck Scanner. Groen betekent dat de persoon beschikt over een geldig testbewijs. Rood betekent dat de persoon niet beschikt over een geldig testbewijs. Een testbewijs is geldig wanneer deze op juiste wijze is ondertekend, ziet op een negatief testresultaat en nog niet is verlopen. Ook krijgt de controleur een set identificerende gegevens te zien (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand) om de identiteit van de gebruikers vast te stellen. Deze set aan identificerende gegevens kan bij een digitaal testbewijs beperkter zijn om de mogelijkheid tot herleidbaarheid van de persoon te verminderen.

7. Belangen bij de gegevensverwerking

De persoon is degene met het grootste belang bij het gebruik van CoronaCheck of het genereren van een papieren testbewijs via coronacheck.nl – deze kan kiezen of hij of zij een testbewijs wil gebruiken om toegang te krijgen tot een gekozen pilot evenement of locatie die onderdeel uitmaakt van de pilotfase.

De controleur heeft een verplichting om enkel personen toe te laten tot het evenement die beschikken over een testbewijs en hebben uit hoofde van die verplichting belang bij het doel waarvoor CoronaCheck wordt ontwikkeld.

Het ministerie van VWS heeft een belang bij het gebruik van CoronaCheck en coronacheck.nl. Dit belang betreft een maatschappelijk belang: dat CoronaCheck een effectief middel is om gecontroleerd uit de lockdown te komen.

8. Verwerkingslocaties

De middelen die nodig zijn voor het beheer van de CoronaCheck app en coronacheck.nl (de configuratieserver en de Signing service) staan in Nederland bij leverancier Prolocation.

Alle andere activiteiten vinden plaats op de smartphone of in de browser van de gebruiker. De controle van het testbewijs vindt plaats op de smartphone of tablet van de controleur.

9. Techniek en methode van gegevensverwerking

CoronaCheck en coronacheck.nl ontvangen de testresultaten op basis van gestandaardiseerde interface / api, wat inhoudt dat het format van de gegevens die door de verstrekker moeten worden aangeleverd juist is. De verantwoordelijkheid voor de juistheid en actualiteit van de gegevens ligt bij de verstrekker.

De conversie van testresultaat naar testbewijs vindt geautomatiseerd plaats waarbij het testresultaat wordt geconverteerd naar een QR-code. Deze QR-code is het testbewijs.

De controleur controleert met CoronaCheck Scanner het testbewijs. De controleur ziet of iemand beschikt over een geldig testbewijs. Hier is sprake van visuele raadpleging van de geldigheid van het testbewijs ('wel geldig testbewijs' / 'geen geldig testbewijs') en krijgt de controleur een set identificerende gegevens te zien (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand). Dit is een geautomatiseerde gegevensverwerking waarmee de QR-code wordt omgezet in een visueel leesbare indicatie van de geldigheid van het testbewijs.

Er is geen sprake van geautomatiseerde besluitvorming, als bedoeld in artikel 22, eerste lid, AVG omdat het besluit over al dan niet toelaten door een controleur wordt genomen.

10. Beveiliging

Bij het ontwerp van de infrastructurele beveiligingsmaatregelen voor de configuratieserver en de signing service van CoronaCheck en coronacheck.nl is uitgegaan van niveau BBN2+ met de maatregelen uit het VIRBI. Daarnaast zijn aanvullende maatregelen getroffen om de beveiliging op te trekken naar het niveau van bescherming tegen het niveau Statelijke Actor, bijvoorbeeld bij de keuze van de toegepaste cryptografie.

11. Juridisch en beleidsmatig kader

In het proces van inladen van het testresultaat in CoronaCheck of coronacheck.nl tot aan het lezen van het testbewijs door de controleur worden persoonsgegevens verwekt. Dit bevat eveneens persoonsgegevens over de gezondheid van een persoon zoals bedoeld in de zin van artikel 9 AVG.

Een testbewijs betreft gegevens over de gezondheid, hetgeen in artikel 4, onderdeel 15, AVG is gedefinieerd als persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.

Op grond van artikel 9, tweede lid, onderdeel a, AVG vormt de uitdrukkelijke toestemming van de betrokkene een doorbrekingsgrond van het verwerkingsverbod uit artikel 9, eerste lid, AVG. Deze grondslag is passend omdat de persoon bij de installatie van de app voor het invoeren van de door de verstrekker ontvangen token op coronacheck.nl expliciet wordt gevraagd kennis te nemen van de privacy voorwaarden en toestemming te geven voor de verwerking van deze gegevens.

12. Bewaartermijnen

Uitgangspunt is dat gegevens zo kort mogelijk worden bewaard. Er gelden verschillende bewaartermijnen voor de gegevens die worden gebruikt binnen CoronaCheck.

- De persoon kan via CoronaCheck een testbewijs genereren. Het testbewijs is maximaal 40 uur[9] geldig (dit tijdstip van testen wordt door de verstrekker meegeleverd). Nadat het testbewijs zijn geldigheid heeft verloren, is deze automatisch onbruikbaar en wordt deze automatisch verwijderd.

[9] Maximale geldigheidsduur kan worden geconfigureerd.

- Een testbewijs is een afgeleide van het testresultaat. Het testresultaat wordt verwijderd uit CoronaCheck zodra het om wordt gezet in een testbewijs. Het testresultaat wordt ook direct verwijderd van de server van VWS nadat het is omgezet in een testbewijs.
- In CoronaCheck Scanner worden geen gegevens vastgelegd.
- Het IP-adres dat in de communicatie van en naar Configuratie Server en de Signing Service wordt gebruikt, wordt door de beheerder 7 dagen bewaard om bij incidenten deze te kunnen onderzoeken. Na deze 7 dagen worden deze automatisch verwijderd. VWS heeft geen toegang tot de IP-adressen.

Ook voor het genereren van een fysiek testbewijs gelden verschillende bewaartermijnen:

- De persoon kan via coronacheck.nl een testbewijs genereren. Het testbewijs is maximaal 40[10] uur geldig (dit tijdstip van testen wordt door de verstrekker meegeleverd). Nadat het testbewijs zijn geldigheid heeft verloren, is deze automatisch onbruikbaar en wordt deze verwijderd uit de browser. Het testbewijs kan ook eerder dan 40 uur verdwijnen wanneer de persoon de browser waarin het testbewijs wordt getoond sluit.
- Het testresultaat wordt ook direct verwijderd van de server van VWS nadat het is omgezet in een testbewijs.
- In de CoronaCheck Scanner app worden geen gegevens vastgelegd.
- Het IP-adres dat in de communicatie van en naar Configuratie Server en de Signing Service wordt gebruikt, wordt door de beheerder maximaal 7 dagen bewaard om bij incidenten deze te kunnen onderzoeken. Na deze 7 dagen worden deze automatisch verwijderd. VWS heeft geen toegang tot de IP-adressen.

Het bewaren van de gegevens bij de verstrekker en bij SON is buiten scope van deze PIA.

[10] Maximale geldigheidsduur kan worden geconfigureerd.

B. Beoordeling rechtmatigheid gegevensverwerkingen

13. Rechtsgrond / Gebruik van bijzondere persoonsgegevens

De gegevens die in het testresultaat, het testbewijs en door middel van de QR-code worden getoond zijn persoonsgegevens in de zin van artikel 4, onderdeel 1, AVG. Daarbij geldt dat het ook bijzondere persoonsgegevens zijn, als bedoeld in art. 4, onderdeel 15 resp. art. 9, eerste lid, AVG. De gegevens die door middel van de QR-code worden getoond bevatten de melding dat een persoon negatief getest is, de datum van de test en bevat een set aan identificerende gegevens (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand). Deze gegevens hebben betrekking op de gezondheidstoestand van de persoon.

Het proces waarbij een QR-code wordt gegenereerd kwalificeert als een verwerking in de zin van artikel 4, onderdeel 2, AVG, omdat bij dit proces persoonsgegevens in de QR-code worden opgenomen. Ook het uitlezen van de QR-code met de set identificerende gegevens (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand) met behulp van de controle app kwalificeert als verwerking zoals bedoeld in de AVG.

Bij het uitlezen van de QR-code en de toegevoegde set identificerende gegevens (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand) is sprake van een geautomatiseerde verwerking van (bijzondere) persoonsgegevens in de zin van artikel 4, onderdeel 2, AVG. Immers, het is de CoronaCheck Scanner app die zorgt voor een vertaling van de QR-code naar een groen of rood scherm. In CoronaCheck Scanner worden geen persoonsgegevens vastgelegd.

Op grond van artikel 9, tweede lid, onderdeel a, AVG vormt de uitdrukkelijke toestemming van de betrokkene een doorbrekingsgrond van het verwerkingsverbod uit artikel 9, eerste lid, AVG. Deze toestemming wordt gegeven door een gebruiker nadat de app op de smartphone van de gebruiker is geïnstalleerd en de gebruiker kennis heeft genomen van de privacyverklaring. Hier wordt ook de nadruk gelegd op het vrijwillige gebruik van de app en de uitdrukkelijke toestemming als grondslag voor de verwerking. Deze grondslag is gekozen wegens de tijdelijke aard van de pilots en in afwachting van het wetsvoorstel dat op 8 maart 2021 ter consultatie is aangeboden.

14. Doelbinding

De gegevensverzameling binnen CoronaCheck en bij het genereren van een papieren testbewijs via coronacheck.nl is minimaal en bevat gegevens (‘drager is negatief getest’, ‘geldigheidsinformatie’ en een beperkte set identificerende gegevens) die nodig zijn om datgene te doen dat van een testbewijs wordt verwacht: het mogelijk maken dat de gebruiker op digitale wijze of op papier een negatief testbewijs kan tonen. Persoonsgegevens worden enkel voor dit doel einde gebruikt.

Daarmee biedt het middel een basisfunctionaliteit die kan worden ingezet op het moment dat er beleidsdoelstellingen bij zijn die de inzet van dit middel legitimeren.

15. Noodzaak en evenredigheid

Het ministerie van VWS werkt er hard aan de samenleving verantwoord te openen. Toegangsbewijzen zijn daar een onderdeel van. Met toegangsbewijzen kunnen sociale, culturele en sportieve locaties in tijden van corona sneller verantwoord open. Met een testbewijs krijgen bezoekers van deze locaties toegang. Met CoronaCheck kunnen bezoekers digitaal hun negatieve

testbewijs tonen om toegang te krijgen tot locaties. Voor het genereren van een fysiek testbewijs kan gebruik worden gemaakt van coronacheck.nl.

Bij het ontwerp van CoronaCheck en coronacheck.nl is het uitgangspunt geweest dat het gebruik van persoonsgegevens tot een minimum moest worden beperkt. Het testbewijs zelf geeft de minimaal benodigde informatie 'de drager hiervan beschikt over een geldig negatief testbewijs' en bevat een minimale set identificerende gegevens om fraude bij het gebruik van CoronaCheck of een fysiek testbewijs te voorkomen. Deze set aan identificerende gegevens wordt, alleen bij een digitaal testbewijs in CoronaCheck, automatisch ingekort wanneer er sprake is van een te hoge kans op herleidbaarheid.

Het gebruik van de eerste letters van voornaam en achternaam en de geboortedag en –maand van persoon zorgt ervoor dat een persoon kan controleren dat het juiste testresultaat wordt opgeslagen op de eigen smartphone of in de eigen browser. Bovendien zorgt de toevoeging van deze set aan identificerende gegevens aan de QR-code ervoor dat het risico op fraude beperkt wordt doordat de controleur middels het identiteitsbewijs kan controleren of het testbewijs ook toebehoort aan de persoon die het testbewijs toont. Het gegevensgebruik is hiermee minimaal en toegespitst op het doel van de verwerking. Door CoronaCheck en het fysieke testbewijs in te zetten kan in een gecontroleerde omgeving getoetst worden of iemand besmet is met COVID-19.

16. Rechten van betrokkene

Het testresultaat / het testbewijs staan op de smartphone of in de browser op het apparaat van de persoon. VWS weet niet dat de persoon over een testbewijs beschikt.

De gegevensstroom is zodanig ontworpen dat VWS niet weet wie er op welk moment over een negatief testbewijs beschikt.

VWS kan de betrokkene niet identificeren, omdat persoonsgegevens bij het tekenen van het testresultaat door de aanbieder en op de signing service verborgen zijn voor VWS. De techniek die wordt gebruikt voor de cryptografische handtekening is dusdanig dat er geen 1:1 relatie te leggen is met een gescande QR-code, ook niet met een kopie van (alle) data uit haar signing service.

De source code en alle technische informatie zijn openbaar beschikbaar via Github.

De personen worden geïnformeerd door middel van een privacy statement over de veiligheid en betrouwbaarheid van CoronaCheck en het genereren van een papieren testbewijs via coronacheck.nl. Dit privacy statement is te vinden op coronacheck.nl en wordt getoond bij het installeren van de CoronaCheck app. De persoon wordt nadrukkelijk gevraagd kennis te nemen van het privacystatement en toestemming te geven voor de verwerking van zijn/haar persoonsgegevens voordat de persoon gebruik kan maken van CoronaCheck of coronacheck.nl.

Voor het uitoefenen van zijn of haar rechten op basis van de AVG verwijst VWS de betrokkene naar de informatiepagina van de Autoriteit Persoonsgegevens.[11] Omdat in het kader van dataminimalisatie de bewaartermijnen dusdanig kort zijn (voor testbewijzen slechts 40 uur vanaf afname coronatest en voor IP-adres maximaal 7 dagen), bestaat de kans dat de gegevens al niet meer aanwezig zijn wanneer de betrokkene een beroep doet op zijn/haar rechten.

[11] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Generieke risico's inzet van testbewijs

In een PIA is het noodzakelijk om stil te staan bij de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Het is hierbij noodzakelijk om daarbij in ieder geval in te gaan op:

- de negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
- de oorsprong van deze gevolgen;
- de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
- de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Specifieke risico's CoronaCheck en fysiek testbewijs

In deze PIA worden de specifieke risico's beschreven die van toepassing zijn op CoronaCheck en het genereren van een papieren testbewijs via coronacheck.nl.

Risico: Misbruik van testbewijzen

Het is voor mensen aantrekkelijk om te kunnen beschikken over een negatief testbewijs. Dit kan het aantrekkelijk maken om misbruik te willen maken van een onecht testbewijs of andermans testbewijs.
Impact: Hoog. Als mensen het testbewijs niet vertrouwen, wordt de app minder gebruikt, wat ten koste gaat van het doel. **Kans:** Klein. Door de set identificerende persoonsgegevens toe te voegen aan het testbewijs neemt de mogelijkheid tot het maken van een vals testbewijs af. Journalisten en hackers kunnen ook de uitdaging zien om de grenzen van het gebruik te verkennen. **Risico:** Medium.
Maatregelen: Het testbewijs is zodanig ontworpen dat misbruik wordt ontmoedigd. Zo kunnen testbewijzen niet zomaar worden gekopieerd of doorgestuurd. Ook zijn maatregelen genomen om grootschalig misbruik door het kopiëren of delen van QR-codes met anderen te bemoeilijken of onmogelijk te maken, bijvoorbeeld door het toevoegen van een bewegende animatie en een set aan identificerende gegevens zowel in als onder de QR-code. CoronaCheck is niet ontworpen om alle scenario's onmogelijk te maken waarbij mensen samenspannen om elkaars testbewijs te gebruiken. In de versie waar deze PIA betrekking op heeft, is er sprake van een beperkte set aan identificerende gegevens (eerste letter voornaam en achternaam, geboortedag en –maand) waartegen bij de controle aan de deur de identiteit kan worden gecontroleerd. Door de toevoeging van deze set identificerende gegevens neemt de kans van dit risico daarmee af. Het is in het belang van de persoon en van de organisator van een activiteit of voorziening om te zorgen dat het testbewijs zorgvuldig wordt gebruikt. Immers: als een gecontroleerde opheffing van de lockdown alsnog leidt tot een oplaaiende besmetting, zal de lockdown opnieuw worden verzwaard.

Ook een zorgvuldige communicatie draagt hieraan bij, door mensen op hun eigen verantwoordelijkheid te wijzen dat in dit stadium de experimenten worden verstoord als niet op een passende manier gebruik wordt gemaakt van CoronaCheck.
Beperking / uitdaging: In het gebruik bestaat een afhankelijkheid van 2 actoren: de persoon zelf en de controleur. Als beide CoronaCheck verantwoord gebruiken, is het frauderisico beperkt.
Impact na maatregelen: Medium. **Kans na maatregelen:** Kans op incidenteel misbruik is laag. Er zullen zeker mensen zijn die dit toch willen uitproberen. **Risico na maatregelen:** Medium.

Risico: Overheid of private partij kan gedrag van persoon volgen

Het digitale testbewijs wordt aangeboden via een app die door het ministerie van VWS wordt gemaakt, op basis van een testresultaat die een teststation wordt gemaakt en een scan van het testbewijs die aan de poort wordt bekeken. Dit kan leiden tot de vrees dat deze partijen kunnen volgen wie er een negatief testbewijs heeft ontvangen en waar iemand is geweest.
Impact: Hoog. Als mensen het CoronaCheck niet vertrouwen, wordt de app minder gebruikt, wat ten laste gaat van het doel. **Kans:** Hoog. Een deel van de bevolking vertrouwt bij voorbaat niet alle middelen die de overheid aanbiedt. **Risico:** Hoog.
Maatregelen: CoronaCheck is zodanig ontworpen dat dit niet het geval is. Personen worden niet gevolgd. Zo weet: • het teststation wel aan wie zij het testresultaat moet geven, maar niet of het testresultaat wordt gebruikt voor een testbewijs en of dit daarna wordt gebruikt om toegang te krijgen tot een evenement of locatie; • het ministerie van VWS weet niet wie een testbewijs heeft gegenereerd; • de controleur heeft geen registratie van testbewijzen. Tijdens het signing proces waarbij het testresultaat omgezet wordt naar het testbewijs verwerkt VWS geautomatiseerd eenmalig de (zeer beperkte) informatie in het testresultaat. Het digitale testbewijs wordt daarbij gerandomiseerd om ervoor te zorgen dat de handtekening niet naar een individu herleidbaar is.
Beperking / uitdaging: Bij de fysieke variant is dit randomiseren technisch niet mogelijk omdat papier statisch is. Als VWS de handtekening zou bijhouden, dan zou VWS bij een tweede keer dat de handtekening wordt gebruikt, kunnen herkennen dat het testbewijs dat met deze handtekening is getekend, hetzelfde is. In de praktijk geldt dat VWS de testbewijzen of handtekeningen niet bewaart.
Impact na maatregelen: Hoog. De maatregelen hebben vooral tot doel om de kans te minimaliseren. **Kans na maatregelen:** Laag. Bij het fysieke testbewijs is de kans nog steeds laag, maar zijn er scenario's denkbaar waarbij kan worden gevolgd waar iemand het testbewijs heeft gebruikt. **Risico na maatregelen:** Laag.

Risico: VWS heeft inzicht in testresultaten en testbewijzen

VWS tekent wel de testbewijzen door de signing service, maar geeft aan geen inzicht in de inhoud van testresultaten of testbewijzen. Hoe weet ik dat zeker?
Impact: Hoog. **Kans:** Laag. **Risico:** Laag.
Maatregelen: In de Signingservice die wordt gebruikt om het testresultaat om te zetten naar een QR-code is geen opslagcapaciteit / database om de getekende bewijzen te kunnen opslaan of inzien. Dit gebeurt dus ook niet. Dit blijkt ook uit de open source code die op GitHub staat.
Beperking / uitdaging: Dit risico treedt alleen op als VWS bewust de code aanpast.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: CoronaCheck houdt bij wie een negatieve test heeft en wie niet

Alle testresultaten en testbewijzen moeten straks bij gebruikers in de CoronaCheck app worden opgeslagen. Kan de overheid dan bijhouden wie negatief is getest en wie niet?
Impact: Hoog. Als mensen het testbewijs niet vertrouwen, wordt de app minder gebruikt, wat ten laste gaat van het doel. **Kans:** Hoog. Een deel van de bevolking vertrouwt niet bij voorbaat alle middelen die de overheid aanbiedt. **Risico**: Hoog.
Maatregelen: Het negatieve testresultaat wordt verstrekt door de partij die heeft getest (op dit moment ingericht door SON). CoronaCheck en coronacheck.nl zetten dit om naar een testbewijs. CoronaCheck en coronacheck.nl bewaren het testbewijs alleen voor zolang als dit geldig is. Als de geldigheidstermijn van 40 uur is verstreken, dan wordt het testbewijs automatisch verwijderd. Een testbewijs blijft altijd alleen op de drager van de persoon. Daarmee is dit risico niet van toepassing. Er is geen sprake van centrale opslag van testresultaten of testbewijzen, door het ministerie van VWS. De source code van CoronaCheck is openbaar en er wordt transparant gecommuniceerd over CoronaCheck. Zo kan iedereen zelf zien dat er geen sprake is van centrale opslag en dat de overheid niet bijhoudt wie negatief is getest en wie niet.
Beperking / uitdaging: Geen.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. Er is geen sprake van centrale opslag van testresultaten of testbewijzen en VWS kan niet zien wie er beschikt over een negatief testbewijs. **Risico na maatregelen:** Laag.

Risico: Een controleur misbruikt de gegevens uit mijn digitale testbewijs

Een controleur die bij een poort testbewijzen controleert ziet van een groot aantal mensen het testbewijs en dus veel gegevens.
Impact: Laag. De controleur ziet alleen de QR-code en de beperkte set identificerende gegevens. **Kans:** Laag. Het is niet aannemelijk dat een controleur gezien het grote aantal personen de set aan identificerende gegevens onthoudt. **Risico:** Laag.
Maatregelen: Regels om misbruik tegen te gaan zijn opgenomen in de gebruikersvoorwaarden voor CoronaCheck Scanner. De controle app die de controleur heeft, legt geen gegevens vast. Bovendien is het niet aannemelijk dat de controleur van een groot aantal personen de persoonsgegevens zal onthouden. De gegevens verdwijnen vanaf de scanner app van de controleur nadat een volgend bewijs is gescand of uiterlijk na 240 seconden.
Beperking / uitdaging: Niet van toepassing.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Verlies van smartphone

Als een persoon zijn of haar smartphone verliest op het moment dat het testresultaat al is gedownload, dan kan deze persoon niet meer het testresultaat gebruiken om een testbewijs te maken en te presenteren.
Impact: Medium, want toegang is niet mogelijk zonder geldig testbewijs. **Kans:** Laag. Het gaat om individuele gevallen. **Risico:** Laag.
Maatregelen: Als de persoon met een nieuwe smartphone zich bij de testaanbieder authenticeert en een testresultaat ophaalt, kan men in de CoronaCheck app met een nieuw testresultaat alsnog een testbewijs genereren. Ook bestaat er de mogelijkheid om nog een fysiek testbewijs te genereren met dezelfde code.
Beperking / uitdaging: Als men niet tijdig over een nieuwe telefoon beschikt en/of zich niet bij de verstrekker kan authenticeren met CoronaCheck.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Er wordt een foutief testresultaat aan VWS geleverd ter ondertekening

Er wordt een foutief testresultaat aan VWS geleverd ter ondertekening
Impact: Laag. **Kans:** Laag. **Risico:** Laag.
Maatregelen: Geen. Er worden voor dit risico geen maatregelen getroffen, want VWS test zelf geen personen. VWS zet enkel het aangeleverde testresultaat van een gecontroleerde testaanbieder om in een testbewijs.
Beperking / uitdaging: N.v.t.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Testresultaat wordt valselijk ondertekend bij signing service

Testresultaat wordt valselijk ondertekend bij signing service
Impact: Hoog. Als dit lukt dan zou een aanval schaalbaar zijn. **Kans:** Laag. **Risico:** Medium.
Maatregelen: Er is cryptografische borging toegevoegd om het valselijk ondertekenen tegen te gaan. CoronaCheck Scanner geeft alleen bij ondertekening met specifiek certificaat via de signing service een groen scherm.
Beperking / uitdaging: N.v.t.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Gebruiker heeft testbewijs in de vorm van QR-code aangepast

Gebruiker heeft testbewijs in de vorm van QR-code aangepast
Impact: Hoog, dit zal men willen gaan uitproberen. **Kans:** Laag. **Risico:** Laag.
Maatregelen: Wijzigingen in de QR-code worden gedetecteerd door het niet kunnen valideren van de VWS ondertekening. De gebruiker heeft geen toegang tot de private key om een nieuwe valide signature te produceren over de gewijzigde testresultaat-data. De nieuwe QR-code zal afgewezen worden door de Corona Scanner app.
Beperking / uitdaging: N.v.t.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: QR-code is niet te scannen in CoronaCheck (foute QR-code in slechte resolutie b.v.)

Risico: QR-code is niet te scannen in CoronaCheck (foute QR-code in slechte resolutie b.v.)
Impact: Medium. **Kans:** Laag. **Risico:** Laag.
Maatregelen: De smartphone waarop CoronaCheck is gedownload moet voldoende schermresolutie hebben en helderheid van het beeldscherm van de smartphone moet voldoende hoog staan. Voor Android geldt dat CoronaCheck werkt vanaf minimaal versie 6 en voor iOS vanaf minimaal versie 11.
Beperking / uitdaging: Een onjuiste QR-code of niet-scanbare QR-code wordt altijd afgewezen, persoon zou geweigerd moeten worden door controleur.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Er worden screenshots van de app doorgestuurd vanaf een ander toestel

Er worden screenshots van de app doorgestuurd vanaf een ander toestel
Impact: Laag. **Kans:** Laag, door de toevoeging van de set identificerende gegevens aan de QR-code. **Risico:** Laag.
Maatregelen: Opgelost door persoonsgegevens in de QR-code op te nemen. Bovendien laat een screenshot van een QR-code in CoronaCheck na 240 seconden niet meer een groen scherm in CoronaCheck Scanner zien. Bij het tonen van een testbewijs in CoronaCheck ziet de controleur een bewegende animatie. Wanneer de animatie niet aanwezig is of niet beweegt kan de controleur zien dat er screenshot is gemaakt van de app. In de gebruikersvoorwaarden voor CoronaCheck Scanner is uitgelegd dat de controleur aan de hand van de animatie kan controleren of er een screenshot van een testbewijs in CoronaCheck is gemaakt.
Beperking / uitdaging: N.v.t.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Er komt een website om QR-codes uit te wisselen of deze te bestellen

Er komt een website om QR-codes uit te wisselen of deze te bestellen.
Impact: Medium. Er is hierbij sprake van een relatief hoge pakkans. Er kunnen kwaadwillenden daarmee niet getest naar het evenement. De verwachting is niet dat dit zeer massaal gebeurt. **Kans:** Medium. Het opzetten kost tijd en inspanning. Daarnaast zal er marketing moeten worden gedaan. **Risico:** Medium.
Maatregelen: Gedeeltelijk opgelost door persoonsgegevens in de QR-code op te nemen.
Beperking / uitdaging: Ook de set aan identificerende gegevens kan onderdeel worden van de illegale handel in QR-codes.

Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Verwarring over roepnaam en officiële naam

Er kan verwarring ontstaan wanneer de eerste letter van iemands voornaam op zijn/haar identiteitsbewijs anders is dan de roepnaam.
Impact: Medium. **Kans:** Laag. **Risico:** Laag.
Maatregelen: In het testbewijs wordt een set met identificerende gegevens toegevoegd om fraude te voorkomen. Dit betreft o.a. testaanbieders moeten duidelijk opnemen dat het testresultaat is gekoppeld aan de officiële namen op ID en niet de roepnaam.
Beperking / uitdaging: N.v.t.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Kleinschalige fraude door doorgeven van smartphone

Doordat personen hun smartphone met daarop een testbewijs kunnen doorgeven aan iemand zonder testbewijs is er een kans op kleinschalige fraude
Impact: Laag. In een enkel geval heeft dat weinig impact op de verwerking van persoonsgegevens. **Kans:** Medium. **Risico:** Laag.
Maatregelen: Dit risico wordt opgelost door **toevoeging van** de **set identificerende gegevens** (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand) **aan** de **QR-code.** De controleur zal aan de hand van een controle van het identiteitsbewijs zien dat de QR-code op de doorgegeven smartphone niet aan deze persoon toebehoort.
Beperking / uitdaging: N.v.t.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: het live doorstreamen van een telefoonscherm

Personen kunnen hun telefoonscherm live doorstreamen
Impact: Hoog. Deze aanval is schaalbaar. **Kans:** Laag. **Risico:** Medium.
Maatregelen: De QR-code bevat zoveel data dat het niet goed te streamen is zonder speciale voorbereidingen.

Beperking / uitdaging: N.v.t.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Mogelijkheid tot genereren meerdere testbewijzen

Het is mogelijk om zowel in CoronaCheck als een fysiek testbewijs te maken met een verstrekt token. Deze token kan meerdere malen gebruikt worden.
Impact: Hoog. Mensen die graag naar een evenement willen, geen test willen of tegen de coronamaatregelen zijn, kunnen op schaal frauderen en mensen besmetten. Een evenement kan een superspreader event worden, omdat er meerdere besmette mensen binnenkomen. Bij breed misbruik is de verplichting tot testen moeilijk verdedigbaar. **Kans:** Hoog. Het is zeer waarschijnlijk dat testbewijzen zullen worden misbruikt. **Risico:** Hoog.
Maatregelen: Door de initialen op te nemen in combinatie met geboortedag en maand en deze bij de ingang structureel te verifiëren tegen een identiteitsbewijs, is het lastiger misbruik te maken.
Beperking / uitdaging: Organisaties controleren het identiteitsbewijs niet.
Impact na maatregelen: Medium. De controles zorgen ervoor dat er misschien wel iemand doorheen glipt, maar niet dat dit massaal kan gebeuren. **Kans na maatregelen:** Medium. Het is zelfs met controle waarschijnlijk dat er bij drukke evenementen mensen door de check heen glippen. Maar dat zal veel minder gebeuren. **Risico na maatregelen:** Medium.

Risico: Kans op herleidbaarheid bij weinig voorkomende set identificerende gegevens

Wanneer een persoon een zeer unieke combinatie van eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand heeft is de kans op herleidbaarheid van de persoon groot.
Impact: Medium. **Kans:** Laag. **Risico:** Medium.
Maatregelen: Bij het genereren van een digitaal testbewijs in CoronaCheck wordt nagegaan (m.b.v. een algoritme) of een set identificerende gegevens zodanig uniek is dat het grote herleidbaarheid van de persoon tot gevolg heeft. Indien dit het geval is wordt één of meer van de vier soorten gegevens die uitmaken van de set identificerende gegevens (eerste letter voornaam, eerste letter achternaam, geboortedag of geboortemaand) uit de set identificerende gegevens die onderdeel uitmaakt van de QR-code gehaald.
Beperking / uitdaging: N.v.t.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

D. Beschrijving voorgenomen maatregelen

In onderdeel C is per risico aangegeven welke maatregelen worden genomen om het risico te beperken. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Onderdeel D beschrijft de overige maatregelen die zijn genomen ter bescherming van de persoonsgegevens van gebruikers. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk. In dit onderdeel wordt ***op hoofdlijnen*** beschreven hoe de cruciale gegevens binnen CoronaCheck zijn beveiligd.

Wat gebeurt bij 'omzetting' van testresultaat naar testbewijs, hoe werkt de cryptografie

Nadat de persoon een coronatest heeft gedaan bij de aangewezen verstrekker, kan hij of zij een ondertekend testresultaat ophalen en in de app of via coronacheck.nl laden. Dit resultaat is ondertekend met een private tekensleutel van de verstrekker.

Voor het ondertekenen van het testresultaat vanuit de signing service wordt gebruik gemaakt van een bestaande implementatie van anoniem ondertekende gegevens volgens het Idemix-protocol. Dit protocol maakt gebruik van een Camenisch-Lysyanskaya (CL) handtekening in combinatie met Zero Knowledge Proofs (ZKP).

Deze CL handtekening wordt elke keer dat een testbewijs gegenereerd wordt gerandomiseerd om ervoor te zorgen dat de handtekening niet naar een individu herleidbaar is. Met andere woorden: de handtekening wordt gerandomiseerd, ofwel “door elkaar gehusseld”. Door een Zero Knowledge Proofs (ZKP) toe te voegen, kan de app zien dat de gerandomiseerde handtekening geldig blijft.

In de ZKPs wordt ook de huidige tijd opgenomen, zodat het testbewijs beperkt geldig is.

Wat gebeurt bij het scannen van de QR door de controleur en wat ziet deze?

De controleur scant het testbewijs (de QR-code) van een persoon. Bij het scannen van de QR-code krijgt de controleur ook de set identificerende gegevens te zien (eerste letter voornaam en eerste letter achternaam, geboortedag en geboortemaand). De ondertekening van de QR- code wordt gecontroleerd door de sleutel die in de CoronaCheck Scanner app aanwezig is. Vervolgens wordt berekend of de handtekening en de ZKPs geldig zijn met behulp van de publieke tekensleutel van VWS. Ook wordt gecontroleerd of het tijdstip dat in de ZKPs is opgenomen, overeenkomt met de huidige tijd met een marge van ongeveer 45 seconden (omdat de handtekening elke anderhalve minuut ververst wordt).

De controleur ziet dus: ‘geldig testbewijs (groen scherm in CoronaCheck Scanner), of ‘geen geldig testbewijs’ (rood scherm CoronaCheck Scanner). In het laatste geval worden daarbij de mogelijke oorzaken genoemd, vooral om te voorkomen dat de controleur er niet automatisch van uitgaat dat de persoon Corona heeft. De controleur kan de persoon niet herkennen aan de uniekheid van de handtekening, omdat deze steeds gerandomiseerd wordt.

Welke maatregelen nemen we om fraude/misbruik te voorkomen?

VWS neemt een groot aantal maatregelen om fraude te voorkomen. Een paar voorbeelden:

- De QR-code is maar beperkt geldig; na een aantal minuten ‘rouleert’ deze ook bij het digitale testbewijs.

- In CoronaCheck (app) worden (bewegende) echtheidskenmerken opgenomen die handmatig en eventueel automatisch gecontroleerd kunnen worden. Deze kenmerken zijn na te maken, maar het maakt het onmogelijk om bijvoorbeeld een screenshot door te sturen of een real-time videoverbinding van het ene scherm naar het andere te gebruiken. Daarmee verhoogt het de barrière voor fraude.
- De set identificerende gegevens welke onderdeel uitmaakt van de QR-code en bij de QR-code wordt getoond draagt bij aan het voorkomen van fraude aan de kant van gebruiker.

Hoe wordt de communicatie van en naar CoronaCheck beveiligd

CoronaCheck en coronacheck.nl (bij het genereren van een testbewijs dat geschikt is om te printen) maken gebruik van transport encryptie (TLS) voor alle verbindingen in combinatie met certificaten van de Nederlandse Public Key Infrastructure (PKI) Overheid en pinning. Dit laatste betekent dat de app alleen contact maakt met servers welke certificaten hebben die uitgegeven zijn door de PKI Overheid.

Daarnaast worden belangrijke configuratie bestanden (waarin bijvoorbeeld de werking van de app beïnvloed kan worden) digitaal getekend. Ook hiervoor worden (alleen) certificaten gebruikt (en geaccepteerd) die onder auspiciën van de Nederlandse haar PKI Overheid uitgegeven zijn met een aantal additionele verificaties. Dit mechanisme wordt zowel gebruikt voor de connecties van de app, alsmede voor de uitslag berichten van de GGD en commerciële partijen. Deze laatsten dienen op een expliciete lijst te staan alvorens geaccepteerd te worden.