Gegevensbeschermingseffectbeoordeling (PIA)

VWS | Directie Informatiebeleid / CIO

PIA CoronaCheck en Coronatoegangsbewijs

Den Haag, 27-05-2021 / Status: Vastgesteld

Vaststelling verwerkingsverantwoordelijke:
Functie: Directeur Programmadirectie Covid-19

Kennisgenomen van FG-advies
Acceptatie restrisico na genomen maatregelen

Datum akkoord: 27 mei 2021

Advies Functionaris voor Gegevensbescherming VWS: 20 mei 2021

Gegevensbeschermingseffectbeoordeling (PIA)

VWS | Directie Informatiebeleid / CIO

PIA CoronaCheck en Coronatoegangsbewijs

Contact:

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

Versie: 1.4, 27 mei 2021

Inhoudsopgave

Inleiding

Deze gegevensbeschermingseffectbeoordeling (hierna: PIA) is opgesteld door het programma 'Realisatie Digitale Ondersteuning' binnen het Ministerie Volksgezondheid, Welzijn en Sport (hierna: VWS) en geldt voor het 'coronatoegangsbewijs'. Het coronatoegangsbewijs is een middel om aan te geven dat deze persoon recent negatief is getest op COVID-19. In deze PIA wordt de voorgenomen verwerking in kaart gebracht en wordt beschreven welke privacybeschermende maatregelen zijn genomen om het coronatoegangsbewijs als middel in te kunnen zetten.

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 de bewegingsvrijheid wordt beperkt door een lockdown, ontstaat de behoefte om op een gecontroleerde manier de samenleving weer te openen. Het coronatoegangsbewijs is een middel wat daarbij kan ondersteunen.

Het coronatoegangsbewijs is een bewijs, met tijdelijke geldigheid, dat een persoon negatief getest is op COVID-19. Dit bewijs kan worden gebruikt om toegang te geven tot specifieke activiteiten en voorzieningen. Een persoon heeft de keuze om een digitaal coronatoegangsbewijs te genereren in CoronaCheck of een coronatoegangsbewijs te genereren dat geschikt is om te printen (fysiek coronatoegangsbewijs) via coronacheck.nl.[1] De inzet van het coronatoegangsbewijs 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 coronatoegangsbewijs gevraagd wordt voor toegang, dienen te controleren of een persoon een geldig coronatoegangsbewijs heeft en gebruiken daarvoor de applicatie CoronaCheck Scanner. Om een coronatoegangsbewijs te verkrijgen is het noodzakelijk dat een persoon zich laat testen op COVID-19. Vervolgens moeten personen, samen met een legitimatiebewijs, het coronatoegangsbewijs tonen aan de controleur bij de ingang van de betreffende activiteit of voorziening. Personen kunnen daarvoor de applicatie CoronaCheck gebruiken of een papieren coronatoegangsbewijs 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 Volksgezondheid, Welzijn en Sport (hierna: de minister) ontwikkeld.

Dit document bevat een PIA op het gebruik van persoonsgegevens voor het coronatoegangsbewijs, de applicaties CoronaCheck en CoronaCheck Scanner en coronacheck.nl, conform artikel 35 van de Algemene Verordening Gegevensbescherming (hierna: AVG). Het uitgangspunt van deze PIA is het voorgenomen gebruik van (persoons)gegevens zoals bekend op 27 mei 2021.

[1] Wanneer in deze PIA 'coronatoegangsbewijs' wordt genoemd betreft dit zowel het digitale coronatoegangsbewijs als het fysieke coronatoegangsbewijs, tenzij dit anders in de PIA wordt genoemd.

A. Beschrijving kenmerken gegevensverwerking

1. Inleiding

Deze PIA ziet op het gebruik van de applicaties CoronaCheck (voor het genereren en gebruiken van een digitaal coronatoegangsbewijs) en CoronaCheck Scanner en het genereren en gebruiken van een papieren coronatoegangsbewijs via coronacheck.nl voor de toegang tot activiteiten en voorzieningen vanaf inwerkingtreding van de Tijdelijke wet coronatoegangsbewijzen. Deze PIA brengt dit proces in kaart en beschrijft welke privacybeschermende maatregelen zijn genomen om het coronatoegangsbewijs als middel in te kunnen zetten.

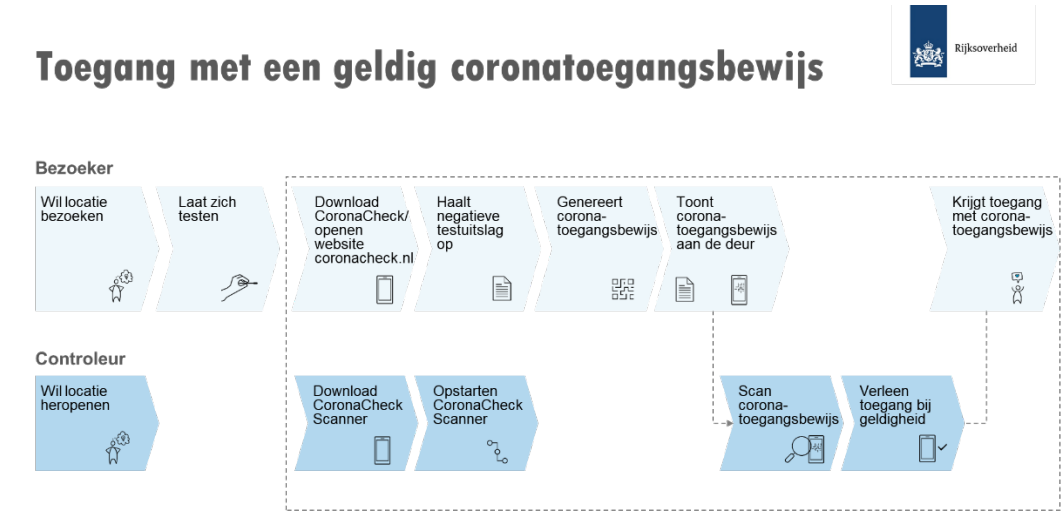
Gebruikte afkortingen

AVG	Algemene Verordening Gegevensbescherming
Controleur	Iemand die de geldigheid van een coronatoegangsbewijs controleert
Coronacheck.nl	De website www.coronacheck.nl waar een persoon een coronatoegangsbewijs kan genereren dat geschikt is om te printen en kan dienen als fysiek coronatoegangsbewijs
Coronatoegangsbewijs	Bewijs gemaakt met negatieve testuitslag dat door de persoon wordt getoond aan een controleur voor toegang tot een activiteit of voorziening.
Minister	De minister van Volksgezondheid, Welzijn en Sport
Ophaalcode	De unieke code die bij testuitslag verstrekt wordt en nodig is om coronatoegangsbewijs te genereren
Persoon	De persoon die een coronatoegangsbewijs wil genereren (digitaal of fysiek) om toegang te krijgen tot een activiteit of voorziening
PIA	Gegevensbeschermingseffectbeoordeling (privacy impact assessment)
Testuitvoerder	Private testaanbieder waar een persoon getest kan worden op COVID-19
Testuitslag	Uitslag van een test op COVID-19 die door de testuitvoerder wordt verstrekt aan een persoon
Verstrekker	Testuitvoerder die een testuitslag verstrekt
VWS	Het ministerie van Volksgezondheid, Welzijn en Sport
Wpg	Wet publieke gezondheid

2. Scope van de PIA

Een wetsvoorstel om coronatoegangsbewijzen op grote schaal in te kunnen zetten bij het heropenen van de samenleving is aangenomen door de Tweede Kamer op 11 mei 2021[2] en is op dezelfde datum ingediend bij de Eerste Kamer[3]. Met dit voorstel wordt de Wet publieke gezondheid (Wpg) gewijzigd. Door preventief te testen en daarvan een coronatoegangsbewijs te verstrekken kunnen verschillende activiteiten en voorzieningen eerder veilig georganiseerd worden. Binnen de scope van deze PIA valt het proces van het ophalen van een testuitslag bij een testuitvoerder tot en met de validatie van het coronatoegangsbewijs door een controleur voor toegang tot een activiteit of voorziening. Buiten de scope van deze PIA valt de gegevensverwerking bij de testuitvoerders (o.a. het maken van de testafspraak, het uitvoeren van de test, het informeren van de persoon over de testuitslag en het digitaal tekenen van de testuitslag door de testuitvoerder). Een coronatoegangsbewijs kan bovendien alleen worden gegenereerd met een negatieve testuitslag (positieve testuitslagen vallen buiten de scope van deze PIA).

Grafisch ziet de scope er als volgt uit, waarbij de stippellijn de scope van deze PIA in figuur 1 weergeeft.



Figuur 1: Grafische weergave scope PIA

2.1. Twee routes – digitaal en fysiek coronatoegangsbewijs

Er zijn twee routes die een persoon kan nemen om een coronatoegangsbewijs te genereren. De eerste route is het gebruik van de applicatie CoronaCheck, waarbij er een digitaal coronatoegangsbewijs wordt gegenereerd. De tweede route is het genereren van een fysiek coronatoegangsbewijs via de website coronacheck.nl. Voor de duidelijkheid zijn beide routes in onderstaande alinea's apart en volledig beschreven.

[2] https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A35807.
[3] https://www.eerstekamer.nl/wetsvoorstel/35807_tijdelijke_wet.

Een persoon heeft de keuze welke route gevolgd wordt en kan van beide routes gebruik maken. Bij een negatieve testuitslag ontvangt de persoon, naast de negatieve testuitslag, ook een ophaalcode van de testuitvoerder om een coronatoegangsbewijs te genereren. Met deze ophaalcode kan zowel een fysiek als een digitaal coronatoegangsbewijs worden gegenereerd. Het omzetten van een testuitslag naar een coronatoegangsbewijs met dezelfde ophaalcode is wel gelimiteerd, hierbij geldt dat er met CoronaCheck maximaal twee keer met dezelfde ophaalcode een coronatoegangsbewijs kan worden gegenereerd. Voor het genereren van een fysiek coronatoegangsbewijs geldt dat dit kan met dezelfde ophaalcode zolang deze geldig is.

2.2. Componenten van CoronaCheck, CoronaCheck Scanner en coronacheck.nl

CoronaCheck bestaat uit de volgende componenten:

- CoronaCheck – dit is de applicatie die de persoon gebruikt om een coronatoegangsbewijs te genereren en vervolgens te presenteren;
- een configuratie server die onder is gebracht bij Prolocation:
    - Voor het beheer van CoronaCheck en CoronaCheck Scanner is een configuratie server actief. Zo wordt bij het opstarten van de applicaties de configuratie opgehaald. Deze configuratie server bevat instellingen zoals de duur van de geldigheid van coronatoegangsbewijzen en sleutels die gebruikt worden voor de beveiliging. Ook bevat de configuratie server een mogelijkheid waarmee, de service om coronatoegangsbewijzen te valideren tijdelijk of permanent beëindigd kan worden. Dit is bijvoorbeeld noodzakelijk als de inzet van CoronaCheck definitief niet meer nodig is.
- een signing service die is ondergebracht bij Prolocation:
    - Met de signing service wordt iedere testuitslag, opgehaald in CoronaCheck, cryptografisch 'getekend' namens de testuitvoerder. Het resultaat hiervan is een ondertekende testuitslag die door CoronaCheck kan worden omgezet in een coronatoegangsbewijs in de vorm van een QR-code.

CoronaCheck Scanner bestaat uit de volgende componenten:

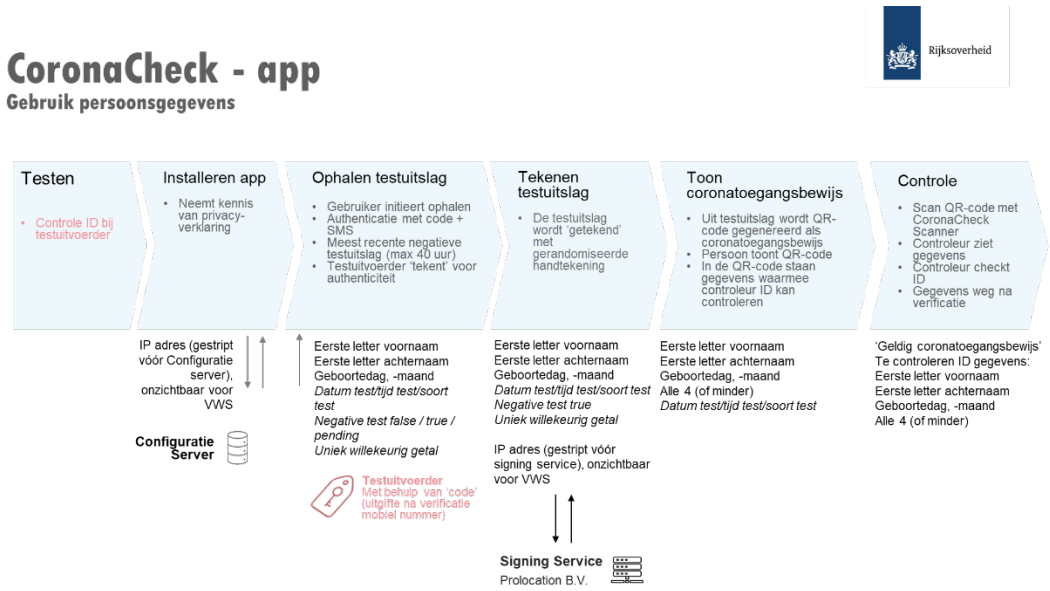
- CoronaCheck Scanner – dit is de applicatie die een controleur gebruikt om te controleren of iemand over een geldig negatief coronatoegangsbewijs beschikt;
- een configuratie server bij Prolocation:
    - Voor het beheer van CoronaCheck en CoronaCheck Scanner is een configuratie server actief. Zo wordt bij het opstarten van de applicaties de configuratie opgehaald. Deze configuratie server bevat instellingen zoals de duur van de geldigheid van coronatoegangsbewijzen en sleutels die gebruikt worden voor de beveiliging. Ook bevat de configuratie server een mogelijkheid waarmee, de service om coronatoegangsbewijzen te valideren tijdelijk of permanent beëindigd kan worden. Dit is bijvoorbeeld noodzakelijk als de inzet van CoronaCheck Scanner definitief niet meer nodig is.

Coronacheck.nl bestaat uit de volgende componenten:

- de website coronacheck.nl – dit is de website die de persoon gebruikt om een coronatoegangsbewijs te genereren en vervolgens te printen;
- een signing service bij Prolocation:
    - met de signing service wordt iedere testuitslag, opgehaald via coronacheck.nl, cryptografisch 'getekend' namens de testuitvoerder. Het resultaat hiervan is een ondertekende testuitslag die door coronacheck.nl kan worden omgezet in een coronatoegangsbewijs in de vorm van een QR-code.

2.3. Beschrijving van het proces voor genereren digitaal coronatoegangsbewijs

Deze alinea beschrijft het proces waarbij gebruik wordt gemaakt van de applicatie CoronaCheck voor het genereren van een digitaal coronatoegangsbewijs. De eerste stap is dat de persoon een test op COVID-19 doet bij een testuitvoerder. 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 figuur 2 een afwijkende kleur.



Figuur 2: Grafische weergave gebruik persoonsgegevens CoronaCheck

Bij de testuitvoerder wordt het emailadres en mobiele nummer van de persoon gevraagd, dit is nodig om (op het moment dat de testuitslag beschikbaar is) de testuitslag met de persoon te kunnen delen. Het gebruik van deze persoonsgegevens valt daarmee buiten scope van deze PIA.

De persoon installeert CoronaCheck op de smartphone[4] via de Apple App Store of de Google Play Store. Na installatie van CoronaCheck, zoekt de applicatie contact met de configuratie server bij Prolocation, om daar de meest recente instellingen en actueel sleutelmateriaal op te halen. Voor het communiceren met de configuratie server wordt een IP-adres gebruikt. Het IP-adres wordt binnen de beheeromgeving niet vastgelegd, deze wordt 'gestript'[5] voordat deze bij de configuratie server komt. De configuratie server krijgt geen externe IP-adressen, maar alleen het interne IP-adres van Prolocation. Het strippen van het IP-adres gebeurt door Prolocation voordat de gegevens naar de configuratie server die is ondergebracht bij Prolocation gaan.

De persoon ontvangt een email met daarin een ophaalcode zodra de negatieve testuitslag beschikbaar is. Vervolgens vult de persoon in CoronaCheck deze ophaalcode in. De persoon krijgt ter controle een SMS op het mobiele telefoonnummer dat is opgegeven bij de testuitvoerder om het ophalen van de testuitslag te bevestigen.

[4] Android vanaf versie 6 en iOS vanaf versie 11.

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

De persoon haalt vervolgens via CoronaCheck de testuitslag op bij de testuitvoerder en plaatst deze in CoronaCheck van de persoon. De testuitvoerder tekent de testuitslag cryptografisch met een private tekensleutel, waarmee CoronaCheck controleert of de testuitslag ook daadwerkelijk van de testuitvoerder afkomstig is. De wijze van tekenen vindt plaats bij de testuitvoerder en is daarmee buiten scope van deze PIA.

Nadat de persoon de negatieve testuitslag heeft opgehaald bij de testuitvoerder kan de persoon ervoor kiezen om van deze testuitslag een coronatoegangsbewijs te maken door op de knop 'Maak QR-code' te klikken. De gegevens worden dan naar de signingservice gestuurd waar de testuitslag wordt getekend. Dit 'tekenen' houdt in dat CoronaCheck de testuitslag voorziet van een gerandomiseerde handtekening. Deze gerandomiseerde handtekening zorgt dat het coronatoegangsbewijs steeds op een andere manier is getekend. Zo kan geen van de betrokken partijen (testuitvoerder, VWS, controleur) volgen waar personen het coronatoegangsbewijs gebruiken.

Ten slotte genereert CoronaCheck een coronatoegangsbewijs. Het coronatoegangsbewijs dat middels CoronaCheck wordt gegenereerd bestaat uit een QR-code 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.

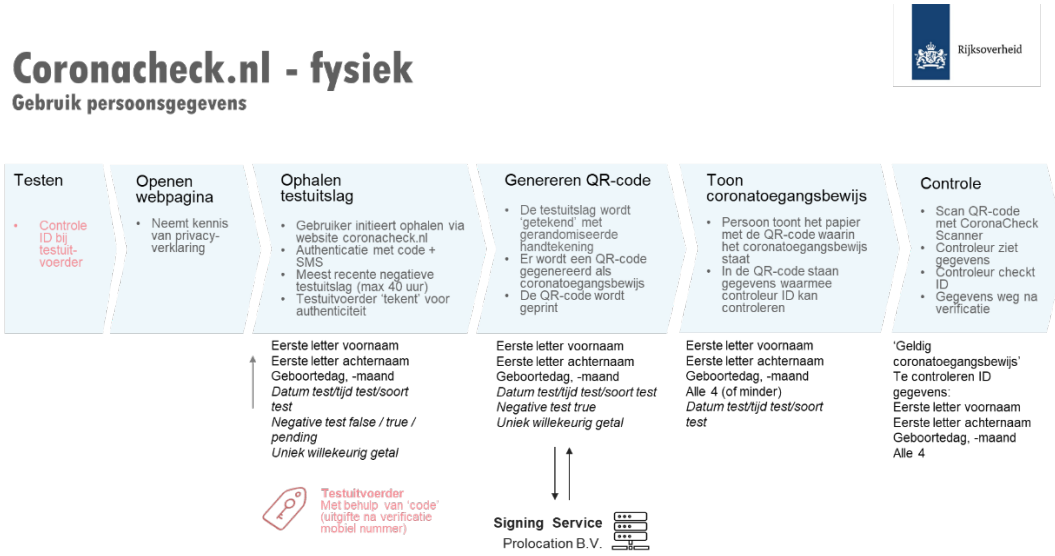
Door middel van privacy by design wordt de set van identificerende gegevens automatisch verder beperkt (dit kan met één of meer van de vier typen identificerende gegevens) wanneer de set identificerende gegevens een te hoge herleidbaarheid van een persoon tot gevolg heeft. Dit is bijvoorbeeld het geval wanneer de eerste letter voornaam en eerste letter achternaam bestaan uit de letters 'X' en 'Y'.[6]

2.4. Beschrijving van het proces voor genereren fysiek coronatoegangsbewijs

Deze alinea beschrijft het proces waarbij gebruik wordt gemaakt van coronacheck.nl voor het genereren van een fysiek coronatoegangsbewijs. Daarvoor is het nodig dat de persoon kan beschikken over een computer met printer, dit kan ook een computer / printer zijn bij bijvoorbeeld familie of buren.

De eerste stap is wederom dat de persoon een test op COVID-19 doet bij een testuitvoerder. 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 figuur 3 een afwijkende kleur. Bij de verstrekker wordt het emailadres en mobiele nummer van de persoon gevraagd, dit is nodig om (op het moment dat de testuitslag beschikbaar is) de testuitslag 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 figuur 3.

[6] Deze oplossing geldt alleen voor het genereren van een digitaal coronatoegangsbewijs in CoronaCheck en niet voor het genereren van een fysiek coronatoegangsbewijs via coronacheck.nl.



Figuur 3: Grafische weergave gebruik persoonsgegevens coronacheck.nl

De persoon ontvangt van de testuitvoerder een email met daarin een ophaalcode zodra de negatieve testuitslag beschikbaar is. Wanneer de persoon gebruik wil maken van een fysiek coronatoegangsbewijs gaat de persoon naar de website coronacheck.nl. Vervolgens vult de persoon op coronacheck.nl deze ophaalcode in. De persoon krijgt ter controle een SMS op het mobiele telefoonnummer dat is opgegeven bij de testuitvoerder om het ophalen van de testuitslag te bevestigen.

Hierna wordt de testuitslag eerst getekend door de verstrekker met een private tekensleutel en daarna door de signing service, zoals ook gebeurt met het digitale coronatoegangsbewijs in CoronaCheck. Dit 'tekenen' houdt in dat de testuitslag is voorzien van een gerandomiseerde handtekening. Deze gerandomiseerde handtekening zorgt dat het coronatoegangsbewijs steeds op een andere manier is getekend. Zo kan geen van de betrokken partijen (testuitvoerder, VWS, controleur) volgen waar mensen dit coronatoegangsbewijs gebruiken.

Het coronatoegangsbewijs dat wordt gegenereerd, via coronacheck.nl, bestaat uit een QR-code 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 coronatoegangsbewijs worden geprint als fysiek coronatoegangsbewijs. De QR-code op het fysieke coronatoegangsbewijs is vergelijkbaar met die van het digitale coronatoegangsbewijs.

2.5. Toegang met coronatoegangsbewijs

Voordat toegang kan worden verkregen tot een activiteit of voorziening wordt het coronatoegangsbewijs (zowel fysiek als digitaal) gecontroleerd door een 'controleur'. De controleur maakt voor de controle op een geldig coronatoegangsbewijs gebruik van de applicatie CoronaCheck Scanner.

CoronaCheck Scanner heeft als functionaliteit het lezen van de QR-code en het op basis daarvan aangeven of deze persoon beschikt over een geldig coronatoegangsbewijs (door middel van een groen scherm bij een geldig coronatoegangsbewijs).

3. Verwerkingen van persoonsgegevens

De volgende gegevens worden gebruikt.

- In de **testuitslag** zijn de volgende gegevens opgenomen:
    - Geregistreerde datum en tijdstip van testen (t.b.v. geldigheidsduur testuitslag), 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 met COVID-19. Een positieve testuitslag 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 de geteste persoon.
    - Digitale handtekening van verstrekker (waarmee ze verantwoording dragen voor het juist uitgegeven negatieve testuitslag en waarmee kan worden gecontroleerd of de gegevens in de testuitslag niet zijn aangepast nadat ze door CoronaCheck zijn ontvangen). De digitale handtekening bevat ook het exacte tijdstip dat die handtekening gezet is.

Deze gegevens worden in de applicatie CoronaCheck op de smartphone van de persoon opgeslagen.

- In het **coronatoegangsbewijs** zijn de volgende gegevens opgenomen:
    - Geregistreerde datum en tijdstip van testen (t.b.v. geldigheidsduur testuitslag), afgerond naar het eerstvolgende hele uur
    - Type test (t.b.v. eventueel te maken onderscheid 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 met COVID-19. Een positieve testuitslag wordt niet via een aparte procedure teruggekoppeld aan de geteste persoon en is volledig buiten scope van deze PIA.
    - Digitale handtekening van de signing service (waarmee kan worden gecontroleerd of de gegevens in de testuitslag niet zijn aangepast nadat ze door de drager zijn ontvangen).
    - Eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand van de geteste persoon.

Voor communicatie met de configuratie server en de signing service van Prolocation wordt het IP-adres gebruikt. Het IP-adres wordt binnen de beheeromgeving niet vastgelegd, deze wordt 'gestript'[7] voordat deze bij de configuratie server of de signing service komt, zodat Prolocation niet ziet welk coronatoegangsbewijs aan welk IP-adres is gekoppeld. De signing server krijgt geen externe IP-adressen, maar alleen het interne IP-adres van Prolocation. Het strippen van het IP-adres gebeurt door Prolocation voordat de gegevens naar de signing server bij Prolocation gaan. Ook VWS krijgt het IP-adres van een persoon niet te zien.

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

Het coronatoegangsbewijs wordt via CoronaCheck gegenereerd en als QR-code op de smartphone van de persoon gepresenteerd en opgeslagen als digitaal coronatoegangsbewijs of in de browser van de persoon via coronacheck.nl getoond om vervolgens als fysiek coronatoegangsbewijs te printen. Een coronatoegangsbewijs wordt met zo min mogelijk persoonsgegevens gegenereerd. De set identificerende gegevens (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand) is in het kader van fraudebestrijding onderdeel van het coronatoegangsbewijs, omdat aan de hand van deze gegevens een controleur kan checken of een coronatoegangsbewijs ook toebehoort aan de persoon die het coronatoegangsbewijs toont.

In de testuitslag en in het coronatoegangsbewijs 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 testuitslag in een coronatoegangsbewijs gaat via de signing service van VWS. De testuitslag wordt hiervoor naar de server bij Prolocation gestuurd. Inherent aan internetcommunicatie is dat hiervoor een IP-adres wordt gebruikt. Het IP-adres wordt binnen de beheeromgeving niet vastgelegd, deze wordt 'gestript'[8] voordat deze bij de signing service komt, zodat de signing service niet ziet welk coronatoegangsbewijs aan welk IP-adres is gekoppeld. De signing server krijgt geen externe IP-adressen, maar alleen het interne IP-adres van Prolocation. Het strippen van het IP-adres gebeurt door Prolocation voordat de gegevens naar de signing server bij Prolocation gaan. Vervolgens wordt de digitale handtekening van de signing service gezet en wordt het coronatoegangsbewijs teruggestuurd naar de persoon. Bij het genereren van een digitaal coronatoegangsbewijs in CoronaCheck wordt op de signing service 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. Het coronatoegangsbewijs wordt vervolgens in CoronaCheck of op via het browserprogramma in coronacheck.nl getoond in de vorm van een QR-code.

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

CoronaCheck Scanner legt van deze controles geen gegevens vast, de applicatie beperkt zich tot het tonen van de genoemde indicatie ('geldig coronatoegangsbewijs'). De gegevens verdwijnen van het scherm bij de eerstvolgende scan of anders uiterlijk na 240 seconden[9] op grond van artikel 6.32 van de Tijdelijke regeling maatregelen covid-19.

4. Doeleinden van de beoogde gegevensverwerking

Het doel van het inzetten van coronatoegangsbewijzen voor toegang tot activiteiten en voorzieningen is om de samenleving op een gecontroleerde wijze uit de lockdown te helpen. Een coronatoegangsbewijs toont aan dat een persoon recent negatief is getest op COVID-19 (maximaal

[8] Door een derde partij (Prolocation) worden deze (externe) IP-adressen vervangen door een intern IP-adres.
[9] Dit is configureerbaar.

40 uur geleden). Door alleen toegang te verlenen aan personen die in het bezit zijn van een coronatoegangsbewijs probeert VWS om uitbraken van COVID-19 door deelname aan een activiteit of bezoek aan een voorziening te voorkomen. Om ook personen die geen gebruik willen of kunnen maken van CoronaCheck de mogelijkheid te bieden een coronatoegangsbewijs te genereren, is er ook de mogelijkheid om een coronatoegangsbewijs via coronacheck.nl te genereren. Dit coronatoegangsbewijs kan vervolgens geprint worden en als fysiek coronatoegangsbewijs getoond worden aan een controleur.

5. Betrokken partijen

Er is een aantal partijen betrokken bij het genereren en gebruiken van een coronatoegangsbewijs met CoronaCheck en van een fysiek coronatoegangsbewijs via coronacheck.nl. Onderstaande toelichting beschrijft welke partijen betrokken zijn en wat de rol van deze partijen is bij het in onderdeel A.2 beschreven proces.

5.1. VWS

CoronaCheck, CoronaCheck Scanner en de website coronacheck.nl zijn ontwikkeld door VWS. De minister is de zelfstandig verwerkingsverantwoordelijke voor de verwerkingen van persoonsgegevens die bij het genereren en gebruiken van een coronatoegangsbewijs via CoronaCheck en coronacheck.nl worden gebruikt op grond van artikel 58re, vijfde lid, Wpg.[10] Binnen CoronaCheck Scanner worden geen persoonsgegevens vastgelegd.

5.2. Persoon

De persoon is degene voor wie een coronatoegangsbewijs gegenereerd wordt. De testuitslag wordt alleen op verzoek van de persoon door CoronaCheck of coronacheck.nl omgezet in een coronatoegangsbewijs.

5.3. Testuitvoerders

Testuitvoerders die testuitslagen aanleveren aan personen ('verstrekkers') zijn betrokken partijen. CoronaCheck en coronacheck.nl halen op verzoek van de persoon bij verstrekkers de negatieve testuitslag op om vervolgens een coronatoegangsbewijs te genereren. Testuitvoerders vervullen de rol van zelfstandig verwerkingsverantwoordelijke voor alle activiteiten die zien op het maken van een testafspraak, het uitvoeren van de test op COVID-19, het communiceren van de testuitslag en ondertekenen van het testresultaat door de signing service. Dit valt daarom buiten de scope van deze PIA.[11]

Wanneer een testuitvoerder wil aansluiten op het in onderdeel A.2. van deze PIA beschreven proces dient de testuitvoerder te voldoen aan de voorwaarden zoals gesteld door VWS in de aansluitvoorwaarden documentatie.[12] Op deze manier worden testuitvoerders aangesloten die voldoen aan de privacy- en security eisen zoals gesteld door VWS.

[10] De uitwerking van de artikelen uit de Wpg in deze PIA is gebaseerd op het gewijzigde voorstel van wet zoals dit op 11 mei 2021 is voorgelegd aan de Eerste Kamer.
[11] Testuitvoerders zijn eventueel aangesloten bij Stichting Open Nederland (SON). SON is geen partij binnen het aansluitproces tussen testuitvoerders en VWS. VWS wisselt geen gegevens uit met SON.
[12] https://www.rijksoverheid.nl/documenten/publicaties/2021/04/29/aansluitvoorwaarden-coronacheck.

5.4. Prolocation

Prolocation beheert de configuratie server waarmee CoronaCheck na installatie contact zoekt om daar de meest recente instellingen en actueel sleutelmateriaal op te halen en heeft hierbij de rol van ontvanger. Prolocation beheert ook de signing service die wordt ingezet om testuitslagen te ondertekenen, welke vervolgens door CoronaCheck of coronacheck.nl worden omgezet in coronatoegangsbewijzen. Testuitvoerders sluiten zelfstandig een overeenkomst met Prolocation voor het ondertekenen van testuitslagen van testen op COVID-19 die door hen zijn afgenomen. Prolocation vervult voor het tekenen van testuitslagen de rol van verwerker voor de testuitvoerders en testuitvoerders de rol van zelfstandig verwerkingsverantwoordelijke.

5.5. Organisatoren van activiteiten en voorzieningen

De organisatoren van activiteiten en voorzieningen, zoals uiteengezet in artikel 58ra, eerste lid, Wpg, kunnen coronatoegangsbewijzen voor toegang vragen aan personen. Met deze organisaties worden geen (persoons)gegevens uitgewisseld en dit valt daarom buiten scope van deze PIA.

5.6. Controleurs

Controleurs scannen met CoronaCheck Scanner het coronatoegangsbewijs van een persoon voor toegang tot een activiteit of voorziening, zoals nader toegelicht in artikel 58ra, eerste lid, Wpg. Controleurs vervullen binnen deze PIA de rol van ontvangers. In CoronaCheck Scanner worden geen persoonsgegevens vastgelegd. De controleur krijgt bij het scannen van een coronatoegangsbewijs te zien of de persoon beschikt over een geldig coronatoegangsbewijs door middel van een groen of een rood scherm in CoronaCheck Scanner. Groen betekent dat de persoon beschikt over een geldig coronatoegangsbewijs. Rood betekent dat de persoon niet beschikt over een geldig coronatoegangsbewijs.

Een controleur controleert aan de hand van het identiteitsbewijs van de persoon of het coronatoegangsbewijs toebehoort aan de persoon die het coronatoegangsbewijs toont. Dit doet de controleur aan de hand van de set identificerende gegevens (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand) die onderdeel uitmaakt van het coronatoegangsbewijs. Deze set aan identificerende gegevens kan bij een digitaal coronatoegangsbewijs beperkter zijn om de mogelijkheid tot herleidbaarheid van de persoon te verminderen.[13]

6. Belangen bij de gegevensverwerking

Personen zijn degenen met het grootste belang bij het gebruik van CoronaCheck of het genereren van een papieren coronatoegangsbewijs via coronacheck.nl. Door middel van het coronatoegangsbewijs kan toegang worden verkregen tot een activiteit of voorziening zoals nader toegelicht in artikel 58ra, eerste lid, Wpg.

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

[13] Dit is een maatregel genomen op het risico, zoals uitgewerkt op pagina 31 van deze PIA, dat de kans op herleidbaarheid groot is wanneer iemand een unieke combinatie aan identificerende gegevens heeft (zoals 'X' en 'Y' als initialen).

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.

7. Verwerkingslocaties

De middelen die nodig zijn als onderdeel van de volledige werking van het systeem om van een testuitslag een coronatoegangsbewijs te maken, dit zijn de configuratieserver en de signing service, staan in Nederland bij leverancier Prolocation.

Alle andere verwerkingen vinden plaats op de smartphone of in de browser van de persoon. De controle van het coronatoegangsbewijs vindt plaats op de smartphone of tablet van de controleur.

8. Techniek en methode van gegevensverwerking

CoronaCheck en coronacheck.nl ontvangen de testuitslagen 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 testuitslag naar coronatoegangsbewijs vindt geautomatiseerd plaats waarbij de testuitslag wordt geconverteerd naar een QR-code. Deze QR-code is het coronatoegangsbewijs.

De controleur controleert met CoronaCheck Scanner het coronatoegangsbewijs. De controleur ziet of iemand beschikt over een geldig coronatoegangsbewijs. Hier is sprake van visuele raadpleging van de geldigheid van het coronatoegangsbewijs (‘wel geldig coronatoegangsbewijs’ / ‘geen geldig coronatoegangsbewijs’) en krijgt de controleur en 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 coronatoegangsbewijs.
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.

9. 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.

10. Juridisch en beleidsmatig kader

Van het ophalen van de testuitslag met behulp van CoronaCheck of via coronacheck.nl tot aan het lezen van het coronatoegangsbewijs door de controleur worden persoonsgegevens verwerkt. Dit zijn eveneens bijzondere persoonsgegevens zoals bedoeld in de zin van artikel 9 AVG.

Een coronatoegangsbewijs betreft namelijk 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.

Voor de verwerking van persoonsgegevens die betrekking hebben op de gezondheid van een persoon geldt op grond van artikel 9 AVG in beginsel een verwerkingsverbod. Deze persoonsgegevens mogen alleen verwerkt worden indien een van de doorbrekingsgronden genoemd in artikel 9, tweede lid, AVG van toepassing is. Op grond van artikel 9, tweede lid, onderdeel g, AVG bieden de Tijdelijke wet coronatoegangsbewijzen en de Tijdelijke regeling maatregelen covid-19 een doorbrekingsgrond van het verwerkingsverbod uit artikel 9, eerste lid, AVG. Daarnaast vormt de vervulling van de taak van algemeen belang, zoals beschreven in de Tijdelijke wet coronatoegangsbewijzen op grond van artikel 6, eerste lid, onderdeel e, AVG de verwerkingsgrondslag voor persoonsgegevens.

De Tijdelijke wet coronatoegangsbewijzen bestaat uit een aantal artikelen die voor tijdelijke duur zijn toegevoegd aan de Wpg. De artikelen 58ra, 58rc, 58rd en 58re Wpg. Tevens is er een ministeriële regeling die de Tijdelijke regeling maatregelen covid-19 wijzigt ten behoeve van het maken van coronatoegangsbewijzen. De gewijzigde wet en regeling bieden de wettelijke grondslag voor de inzet van coronatoegangsbewijzen zoals beschreven in onderdeel A.2. van deze PIA.

Coronatoegangsbewijzen moeten uitgevraagd worden indien op grond van artikel 58ra, eerste lid, Wpg regels zijn gesteld op de volgende terreinen:
- cultuur;
- evenementen;
- georganiseerde jeugdactiviteiten;
- horeca; of
- sport.[14]

Op grond van artikel 6.27 van de Tijdelijke regeling maatregelen covid-19 bevat een testuitslag zoals deze door de teststations wordt verstrekt de volgende gegevens:
- de naam en de geboortedatum van de geteste persoon;
- het type test dat is uitgevoerd;
- de datum en het tijdstip van de afname van de test; en
- de uitslag van de uitgevoerde test

Nadat een persoon een verzoek doet in CoronaCheck of via coronacheck.nl om een coronatoegangsbewijs te genereren worden op grond van artikel 58rd, eerste lid, Wpg en artikel 6.31, eerste lid, van de Tijdelijke regeling maatregelen covid-19 de volgende gegevens verstrekt door de testuitvoerder:
- de initialen, de geboortemaand en de geboortedag van de geteste persoon;
- het type test dat is uitgevoerd;
- de datum en het op hele uren afgeronde tijdstip van afname van de test;
- de uitslag van de uitgevoerde test; en
- een code (de ophaalcode) voor het opvragen van de gegevens.

Een digitaal coronatoegangsbewijs kan vervolgens worden gegenereerd in CoronaCheck op grond van artikel 58re, eerste lid, onder a, onder 1° Wpg jo. artikel 6.31, tweede lid, van de Tijdelijke regeling maatregelen covid-19.

[14] Op grond van artikel 58ra, derde lid, Wpg kan bij of krachtens algemene maatregel van bestuur worden bepaald dat de inzet van coronatoegangsbewijzen ook van toepassing is op het terrein van beroepsonderwijs of hoger onderwijs.

Voor het scannen van een digitaal of fysiek coronatoegangsbewijs met CoronaCheck Scanner bieden artikel 58re, derde lid Wpg en artikel 6.231, vierde lid, van de Tijdelijke regeling maatregelen covid-19 de wettelijke grondslag.

Artikel 58re, eerste lid, Wpg noemt de grondslag voor het tonen van een digitaal coronatoegangsbewijs met CoronaCheck of een fysiek coronatoegangsbewijs op papier. Voor een fysiek coronatoegangsbewijs gelden op grond van artikel 6.28 van Tijdelijke regeling maatregelen covid-19 de volgende eisen:

- de QR-code moet zijn voorzien van een elektronische handtekening op basis van een door de minister beschikbaar gesteld digitaal certificaat. Dit gebeurt door middel van de ondertekening van de signing service.
- de QR-code bevat de volgende gegevens:
    - de intialen, de geboortemaand en de geboortedag van de geteste persoon;
    - de datum en het op hele uren afgeronde tijdstip vanaf welke het coronatoegangsbewijs geldig is; en de duur van de geldigheid van het coronatoegangsbewijs.
- de QR-code moet zodanig zijn samengesteld dat deze met CoronaCheck Scanner kan worden gelezen en dat CoronaCheck Scanner toont of een QR-code een geldig coronatoegangsbewijs bevat en indien dit het geval is worden ook de gegevens getoond zoals in de vorige bulletpoint benoemd.

Een coronatoegangsbewijs is op grond van artikel 6.29 van de Tijdelijke regeling maatregelen covid-19 geldig indien:

- het coronatoegangsbewijs betrekking heeft op de persoon die de deelname of toegang wenst;
- het coronatoegangsbewijs betrekking heeft op het type test dat krachtens de wet is voorgeschreven voor de deelname of toegang;
- de uitslag van de uitgevoerde test op COVID-19 negatief is; en
- op het moment van aanvang van de deelname of toegang niet meer dan veertig uren zijn verstreken sinds het tijdstip van afname van de test.

Artikel 6.30 van de Tijdelijke regeling maatregelen covid-19 bevat de verplichting voor een controleur om de persoon te controleren op zijn of haar identiteit bij activiteiten of voorzieningen waarvoor een coronatoegangsbewijs gevraagd wordt.

11. 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 coronatoegangsbewijs genereren. Het coronatoegangsbewijs is maximaal 40 uur[15] geldig (dit tijdstip van testen wordt door de verstrekker meegeleverd). Nadat het coronatoegangsbewijs zijn geldigheid heeft verloren, is deze automatisch onbruikbaar en wordt deze automatisch verwijderd.
- Een coronatoegangsbewijs is een afgeleide van de testuitslag. De testuitslag wordt verwijderd uit CoronaCheck zodra het om wordt gezet in een coronatoegangsbewijs. De testuitslag wordt ook direct verwijderd van de server bij Prolocation nadat het is omgezet in een coronatoegangsbewijs.
- In CoronaCheck Scanner worden geen gegevens vastgelegd.

[15] Maximale geldigheidsduur kan worden geconfigureerd.

- 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 incidenten 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 coronatoegangsbewijs gelden verschillende bewaartermijnen:

- De persoon kan via coronacheck.nl een coronatoegangsbewijs genereren. Het coronatoegangsbewijs is maximaal 40[16] uur geldig (dit tijdstip van testen wordt door de verstrekker meegeleverd). Nadat het coronatoegangsbewijs zijn geldigheid heeft verloren, is deze automatisch onbruikbaar en wordt deze verwijderd uit de browser. Het coronatoegangsbewijs kan ook eerder dan 40 uur verdwijnen wanneer de persoon de browser waarin het coronatoegangsbewijs wordt getoond sluit.
- De testuitslag wordt ook direct verwijderd van de server bij Prolocation nadat het is omgezet in een coronatoegangsbewijs.
- 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 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 is buiten scope van deze PIA.

[16] Maximale geldigheidsduur kan worden geconfigureerd.

B. Beoordeling rechtmatigheid gegevensverwerkingen

12. Rechtsgrond / Gebruik van bijzondere persoonsgegevens

De gegevens die in de testuitslag, het coronatoegangsbewijs 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 gezondheid 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 CoronaCheck Scanner 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 CoronaCheck Scanner 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 g, AVG en artikel 6, eerste lid, onderdeel e, AVG bieden de Tijdelijke wet coronatoegangsbewijzen en de Tijdelijke regeling maatregelen covid-19 een doorbrekingsgrond van het verwerkingsverbod uit artikel 9, eerste lid, AVG. De verwerking van gezondheidsgegevens is noodzakelijk om het doel van de inzet van coronatoegangsbewijzen te kunnen bereiken, namelijk het aantonen dat een persoon op het moment van afname van de test niet besmet was met COVID-19 en de persoon op basis van dit gegeven toegang te verlenen tot een activiteit of voorziening. De Tijdelijke wet coronatoegangsbewijzen en de Tijdelijke regeling maatregelen covid-19 bieden de wettelijke grondslag voor de verwerking van (bijzondere) persoonsgegevens, zoals uitgewerkt in onderdeel A.10 van deze PIA.

13. Doelbinding

De verwerking van persoonsgegevens binnen CoronaCheck en bij het genereren van een papieren coronatoegangsbewijs via coronacheck.nl is minimaal en bevat gegevens (‘drager is negatief getest’, ‘geldigheidsinformatie’ en een beperkte set identificerende gegevens) die nodig zijn om te voldoen aan de eisen zoals gesteld in de Tijdelijke wet coronatoegangsbewijzen en de Tijdelijke regeling maatregelen covid-19. Persoonsgegevens worden enkel voor dit doel einde gebruikt.

14. Noodzaak en evenredigheid

Met de inzet coronatoegangsbewijzen kunnen activiteiten en voorzieningen in tijden van COVID-19 sneller verantwoord plaatsvinden. Met CoronaCheck kunnen personen digitaal hun coronatoegangsbewijs tonen om toegang te krijgen tot activiteiten en voorzieningen. Voor het genereren van een fysiek coronatoegangsbewijs 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 coronatoegangsbewijs zelf geeft de minimaal benodigde informatie 'de drager hiervan beschikt over een geldig coronatoegangsbewijs' en bevat een minimale set identificerende gegevens om fraude bij het gebruik van CoronaCheck of een fysiek coronatoegangsbewijs te voorkomen. Deze set aan identificerende gegevens wordt, alleen bij een digitaal coronatoegangsbewijs 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 de juiste testuitslag 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 coronatoegangsbewijs ook toebehoort aan de persoon die het coronatoegangsbewijs toont. Het gegevensgebruik is hiermee minimaal en toegespitst op het doel van de verwerking. Door CoronaCheck en het fysieke coronatoegangsbewijs in te zetten kan in een gecontroleerde omgeving getoetst worden of iemand besmet is met COVID-19.

15. Rechten van betrokkene

De personen worden geïnformeerd door middel van een privacy statement over CoronaCheck en het genereren van een papieren coronatoegangsbewijs via coronacheck.nl. Dit privacy statement is te vinden op coronacheck.nl en wordt getoond bij het installeren van CoronaCheck. De source code van CoronaCheck en CoronaCheck Scanner en alle technische informatie zijn bovendien openbaar beschikbaar via GitHub.

De testuitslagen het coronatoegangsbewijs staan op de smartphone of in de browser op het apparaat van de persoon. VWS kan de betrokkene niet identificeren, en weet dus niet wie er over een coronatoegangsbewijs beschikt, omdat persoonsgegevens bij het tekenen van de testuitslag door de testuitvoerder 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. Desondanks hebben personen het recht om hun rechten op basis van de AVG uit te oefenen.

Voor het uitoefenen van zijn of haar rechten op basis van de AVG verwijst VWS de betrokkene naar de informatiepagina van de Autoriteit Persoonsgegevens.[17] Omdat in het kader van dataminimalisatie de bewaartermijnen dusdanig kort zijn (voor coronatoegangsbewijzen slechts 40 uur vanaf afname coronatest en voor IP-adres maximaal 7 dagen), bestaat de kans dat de gegevens niet meer aanwezig zijn wanneer een betrokkene een beroep doet op de rechten voor betrokkenen uit de AVG.

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

C. Beschrijving en beoordeling risico's voor de betrokkenen

16. Generieke risico's inzet van coronatoegangsbewijs

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.

17. Specifieke risico's CoronaCheck en fysiek coronatoegangsbewijs

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

Risico: Misbruik van coronatoegangsbewijzen

Het is voor personen aantrekkelijk om te kunnen beschikken over een coronatoegangsbewijs. Dit kan het aantrekkelijk maken om misbruik te willen maken van een onecht coronatoegangsbewijs of andermans coronatoegangsbewijs. Hierdoor kan toegang tot een activiteit of voorziening worden verkregen zonder dat iemand recent negatief is getest op COVID-19.
Impact: Hoog. Als mensen het coronatoegangsbewijs niet vertrouwen, worden CoronaCheck en coronacheck.nl minder gebruikt, wat ten koste gaat van het doel. **Kans:** Klein. Door de set identificerende persoonsgegevens toe te voegen aan het coronatoegangsbewijs neemt de mogelijkheid tot het maken van een vals coronatoegangsbewijs af. Journalisten en hackers kunnen ook de uitdaging zien om de grenzen van het gebruik te verkennen. **Risico:** Medium.
Maatregelen: Het coronatoegangsbewijs is zodanig ontworpen dat misbruik wordt ontmoedigd. Zo kunnen coronatoegangsbewijzen 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 aparte regel onder de QR-code. CoronaCheck is niet ontworpen om alle scenario's onmogelijk te maken waarbij personen samenspannen om elkaars coronatoegangsbewijs te gebruiken of proberen gebruik te maken van een nep coronatoegangsbewijs. 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 coronatoegangsbewijs 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, maar er blijft een kans bestaan op pogingen tot misbruik van coronatoegangsbewijzen. **Risico na maatregelen:** Medium.

Risico: Overheid of private partij kan gedrag van persoon volgen

Het digitale coronatoegangsbewijs wordt aangeboden via een applicatie die door VWS wordt gemaakt, op basis van een testuitslag die door een testuitvoerder wordt verstrekt. Vervolgens wordt een scan van het coronatoegangsbewijs bekeken voordat toegang wordt verleend aan een persoon tot een activiteit of voorziening. Het gebruik van een digitaal middel dat ontwikkeld is door VWS kan leiden tot de vrees dat de overheid of testuitvoerder kan volgen wie er een coronatoegangsbewijs heeft ontvangen en waar iemand is geweest.
Impact: Hoog. Als mensen CoronaCheck niet vertrouwen, wordt de applicatie minder gebruikt, wat ten koste gaat van het doel. **Kans:** Hoog. Het is niet vanzelfsprekend dat personen middelen vertrouwen die door de overheid zijn ontwikkeld. **Risico:** Hoog.
Maatregelen: CoronaCheck is zodanig ontworpen dat de overheid of een private partij een persoon niet kan volgen. Zo weet: - de testuitvoerder wel aan wie zij de testuitslag moet geven, maar niet of de testuitslag wordt gebruikt voor een coronatoegangsbewijs en of dit daarna wordt gebruikt om toegang te krijgen tot een activiteit of voorziening; - VWS weet niet wie een coronatoegangsbewijs heeft gegenereerd; - de controleur heeft geen registratie van coronatoegangsbewijzen. Tijdens het signing proces waarbij de testuitslag omgezet wordt naar het coronatoegangsbewijs verwerkt Prolocation geautomatiseerd eenmalig de (zeer beperkte) informatie in de testuitslag. Het digitale coronatoegangsbewijs 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 coronatoegangsbewijs dat met deze handtekening is getekend, hetzelfde is. Dit gaat echter niet op want, in de praktijk geldt dat VWS de coronatoegangsbewijzen 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 coronatoegangsbewijs is de kans nog steeds laag, maar zijn er scenario's denkbaar waarbij kan worden gevolgd waar iemand het coronatoegangsbewijs heeft gebruikt. **Risico na maatregelen:** Laag.

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

Testuitslagen en digitale coronatoegangsbewijzen moeten straks bij personen op de smartphone in CoronaCheck worden opgeslagen. Dit kan zorgen voor vrees dat de overheid bijhoudt wie negatief is getest en wie niet, wat tot gevolg kan hebben dat personen CoronaCheck niet vertrouwen en daarom niet gebruiken.
Impact: Hoog. Als mensen het coronatoegangsbewijs niet vertrouwen, wordt CoronaCheck en coronacheck.nl minder gebruikt, wat ten laste gaat van het doel. **Kans:** Hoog. Het is niet vanzelfsprekend dat personen middelen vertrouwen die door de overheid zijn ontwikkeld. **Risico**: Hoog.
Maatregelen: De negatieve testuitslag wordt verstrekt door de testuitvoerders. CoronaCheck en coronacheck.nl zetten dit om naar een coronatoegangsbewijs. CoronaCheck en coronacheck.nl bewaren het coronatoegangsbewijs alleen voor zolang als dit geldig is. Als de geldigheidstermijn van 40 uur is verstreken, dan wordt het coronatoegangsbewijs automatisch verwijderd. Een coronatoegangsbewijs blijft altijd alleen op de smartphone van de persoon en wordt dus niet op een (centrale) server opgeslagen. Omdat er geen sprake van centrale opslag van testuitslagen of coronatoegangsbewijzen door VWS is het niet mogelijk dat CoronaCheck of VWS bijhoudt wie negatief getest is op COVID-19. 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 testuitslagen of coronatoegangsbewijzen en VWS kan niet zien wie er beschikt over een coronatoegangsbewijs. **Risico na maatregelen:** Laag.

Risico: Een controleur misbruikt de gegevens uit het coronatoegangsbewijs

Een controleur die coronatoegangsbewijzen controleert ziet van een groot aantal mensen het coronatoegangsbewijs en dus veel persoonsgegevens. De controleur kan misbruik maken van deze gegevens, wat een risico voor de rechten en vrijheden van personen tot gevolg kan hebben.
Impact: Laag. De controleur ziet alleen de QR-code en de beperkte set identificerende gegevens (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand).

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 bij het scannen van coronatoegangsbewijzen tegen te gaan zijn opgenomen in de gebruikersvoorwaarden voor CoronaCheck Scanner. Voordat gebruik kan worden gemaakt van CoronaCheck Scanner dient akkoord te worden gegaan met de regels zoals gesteld in de gebruikersvoorwaarden voor CoronaCheck Scanner. In CoronaCheck Scanner worden daarnaast geen gegevens vastgelegd. CoronaCheck Scanner wordt alleen gebruikt om een coronatoegangsbewijs te scannen en vervolgens al dan niet toegang te verlenen aan een persoon tot een activiteit of voorziening. Bovendien is het niet aannemelijk dat de controleur van een groot aantal personen de persoonsgegevens zal onthouden. Daarnaast betreft het een beperkte set aan identificerende gegevens, wat inhoudt dat alleen (of zelfs minder dan) de eerste letter voornaam, de eerste letter achternaam, geboortedag en geboortemaand aan de controleur worden getoond. De gegevens verdwijnen vanaf CoronaCheck Scanner nadat een volgend bewijs is gescand of uiterlijk na 240 **seconden op grond van artikel 6.**32 **van** de Tijdelijke regeling maatregelen covid-19**.**
Beperking / uitdaging: Niet van toepassing.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Geen toegang tot activiteit of voorziening door verlies van smartphone

Voor het tonen van een digitaal coronatoegangsbewijs downloadt een persoon CoronaCheck op zijn of haar smartphone. Als een persoon de smartphone verliest op het moment dat de testuitslag al is gedownload, kan deze persoon niet meer de testuitslag gebruiken om een coronatoegangsbewijs te maken om te presenteren. Zonder coronatoegangsbewijs kan geen toegang worden verkregen door in de Tijdelijke wet coronatoegangsbewijzen aangewezen activiteiten en voorzieningen.
Impact: Medium, want toegang is niet mogelijk zonder geldig coronatoegangsbewijs. **Kans:** Laag. Het gaat om individuele gevallen. **Risico:** Laag.
Maatregelen: Als de persoon zich met een nieuwe smartphone bij de testuitvoerder authentiseert en een testuitslag opnieuw ophaalt, kan men in CoronaCheck met een nieuwe testuitslag alsnog een coronatoegangsbewijs genereren. Ook bestaat er de mogelijkheid om nog een fysiek coronatoegangsbewijs te genereren met dezelfde ophaalcode. Het gebruiken van dezelfde ophaalcode voor het genereren van een coronatoegangsbewijs in CoronaCheck is twee keer mogelijk en voor het genereren van een fysiek coronatoegangsbewijs zolang de ophaalcode geldig is (40 uur).
Beperking / uitdaging: Als men niet tijdig over een nieuwe telefoon beschikt en/of zich niet bij de verstrekker kan authentiseren met CoronaCheck.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag.

Risico na maatregelen: Laag.

Risico: Er wordt een foutieve testuitslag geleverd ter ondertekening

Een testuitslag wordt geleverd aan de signing service ter ondertekening. Hierbij bestaat het risico dat er een foutieve testuitslag wordt geleverd ter ondertekening. Dit kan ertoe leiden dat de testuitslag niet ondertekend kan worden en geen coronatoegangsbewijs kan worden gegenereerd.
Impact: Laag. **Kans:** Laag. **Risico:** Laag.
Maatregelen: Geen. Er worden voor dit risico geen maatregelen getroffen, want VWS ondertekent de testuitslagen niet, dit doet Prolocation.
Beperking / uitdaging: N.v.t.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Testuitslag wordt valselijk ondertekend bij signing service

Een testuitslag wordt voor omzetting naar een coronatoegangsbewijs ondertekend in de signing service. Her risico bestaat dat de testuitslag valselijk ondertekend wordt in de signing service. Dit kan problemen veroorzaken bij het scannen van een coronatoegangsbewijs met CoronaCheck Scanner, waardoor een persoon mogelijk geen toegang krijgt tot een evenement of locatie.
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: Persoon vervalst coronatoegangsbewijs in de vorm van QR-code

Voordat een persoon toegang krijgt tot een activiteit of voorziening dient deze een coronatoegangsbewijs in de vorm van een QR-code te tonen aan een controleur. Een persoon kan het coronatoegangsbewijs in de vorm van QR-code vervalsen waardoor toegang wordt verkregen tot een activiteit of voorziening zonder een recente negatieve testuitslag. Dit kan

leiden tot een hogere besmettingskans voor andere personen die toegang hebben tot de activiteit of voorziening.
Impact: Hoog, op deze manier kunnen personen die niet in bezit zijn van een coronatoegangsbewijs toegang verkrijgen tot een activiteit of een voorziening. **Kans:** Laag. **Risico:** Laag.
Maatregelen: Wijzigingen in de QR-code worden gedetecteerd door het niet kunnen valideren van de VWS ondertekening. De persoon heeft geen toegang tot de private key om een nieuwe valide signature te produceren over de gewijzigde testuitslag-data. De nieuwe QR-code zal afgewezen worden door CoronaCheck Scanner.
Beperking / uitdaging: N.v.t.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Digitale coronatoegangsbewijs in CoronaCheck kan niet worden gescand

Voor het verkrijgen van toegang tot in de Tijdelijke wet coronatoegangsbewijzen aangewezen activiteiten en voorzieningen is een coronatoegangsbewijs vereist. Het digitale coronatoegangsbewijs in CoronaCheck kan niet worden gescand door bijvoorbeeld een slechte resolutie van de smartphone van de persoon. Hierdoor kan het coronatoegangsbewijs niet gescand worden door CoronaCheck Scanner en krijgt een persoon mogelijk geen toegang tot een activiteit of voorziening.
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 door CoronaCheck Scanner. Het is aan de controleur om te bepalen of een persoon toegang krijgt tot een activiteit of voorziening.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Er worden screenshots van het coronatoegangsbewijs in CoronaCheck doorgestuurd naar een ander toestel

Het digitale coronatoegangsbewijs wordt in de vorm van een QR-code getoond in CoronaCheck. Screenshots van het coronatoegangsbewijs in CoronaCheck kunnen worden doorgestuurd naar een ander toestel, waardoor een persoon zonder geldig coronatoegangsbewijs mogelijk toegang krijgt tot een activiteit of voorziening. Dit kan een verhoogde kans op een uitbraak van COVID-19 veroorzaken.
Impact: Laag.

Kans: Laag, door de toevoeging van de set identificerende gegevens aan de QR-code is de kans op fraude verkleind. **Risico:** Laag.
Maatregelen: Dit risico is opgelost door persoonsgegevens in de QR-code en als regel onder de QR-code op te nemen. Bovendien laat een screenshot van een coronatoegangsbewijs in CoronaCheck na 240 seconden niet meer een groen scherm in CoronaCheck Scanner zien. Bij het tonen van een coronatoegangsbewijs 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 een coronatoegangsbewijs in CoronaCheck. 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 coronatoegangsbewijs 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

Een coronatoegangsbewijs wordt in de vorm van een QR-code door een persoon getoond aan een controleur. Er bestaat een risico dat er een website wordt ontwikkeld om QR-codes uit te wisselen of deze te bestellen, waardoor personen mogelijk toegang krijgen tot een activiteit of voorziening zonder dat zij beschikken over een recente negatieve testuitslag. Dit kan een verhoogde kans op een uitbraak van COVID-19 binnen een activiteit of voorziening veroorzaken.
Impact: Medium. Er kunnen kwaadwillenden daarmee naar de activiteit of voorziening zonder dat zij negatief getest zijn op COVID-19. **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. Er is bovendien sprake van een relatief hoge pakkans doordat wijzigingen in de QR-code worden gedetecteerd door het niet kunnen valideren van de VWS ondertekening. De persoon heeft geen toegang tot de private key om een nieuwe valide signature te produceren over de gewijzigde testuitslag-data. De nieuwe QR-code zal afgewezen worden door CoronaCheck Scanner.
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

Bij het aanmelden voor een test op COVID-19 geeft de persoon zijn of haar naam op. Er kan verwarring ontstaan wanneer er bij het aanmelden voor een test op COVID-19 de eerste letter

van iemands voornaam op zijn/haar identiteitsbewijs anders is dan de roepnaam. In dat geval komt de set identificerende gegevens niet overeen met het identiteitsbewijs van de persoon. Hierdoor zal het voor de controleur lijken alsof het coronatoegangsbewijs niet toebehoort aan de persoon die het coronatoegangsbewijs toont.
Impact: Medium. **Kans:** Laag. **Risico:** Laag.
Maatregelen: In het coronatoegangsbewijs wordt een set met identificerende gegevens toegevoegd om fraude te voorkomen. Het is belangrijk dat deze set aan identificerende gegevens overeenkomt met de gegevens op het identiteitsbewijs van de persoon. Testuitvoerders moeten duidelijk opnemen dat de testuitslag is gekoppeld aan de officiële namen op het identiteitsbewijs en niet de roepnaam om verwarring hierover te voorkomen.
Beperking / uitdaging: N.v.t.
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. **Risico na maatregelen:** Laag.

Risico: Fraude door doorgeven van smartphone

Een digitaal coronatoegangsbewijs wordt getoond in CoronaCheck op de smartphone van de persoon. Doordat personen hun smartphone met daarop een coronatoegangsbewijs kunnen doorgeven aan iemand zonder coronatoegangsbewijs is er een kans op kleinschalige fraude. Hierdoor kan een persoon toegang krijgen tot een activiteit of voorzieningen zonder dat de persoon recent negatief getest is op COVID-19, waardoor er binnen de activiteit of voorziening een uitbraak kan ontstaan.
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 coronatoegangsbewijs in CoronaCheck

In CoronaCheck worden digitale coronatoegangsbewijzen getoond. Personen kunnen hun telefoonscherm live doorstreamen waarin een coronatoegangsbewijs in CoronaCheck te zien is. Hierdoor bestaat de kans dat een persoon die niet beschikt over een negatief coronatoegangsbewijs toegang krijgt tot een activiteit of voorziening, wat een uitbraak van COVID-19 tot gevolg zou kunnen hebben.
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 coronatoegangsbewijzen

Een coronatoegangsbewijs wordt gegenereerd door middel van een ophaalcode. Het is mogelijk om zowel in CoronaCheck als een fysiek coronatoegangsbewijs te maken met een verstrekte ophaalcode. Deze ophaalcode kan dus meerdere malen gebruikt worden. Dit kan tot gevolg hebben dat verschillende personen met dezelfde ophaalcode een coronatoegangsbewijs genereren en dat hiermee toegang tot een activiteit of voorziening wordt verkregen door personen die niet recent negatief getest zijn op COVID-19.
Impact: Hoog. Een activiteit of voorziening 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 coronatoegangsbewijzen zullen worden misbruikt. **Risico:** Hoog.
Maatregelen: Door in de QR-code de set identificerende persoonsgegevens (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand) op te nemen en deze bij de ingang structureel te controleren door middel van het vragen van een identiteitsbewijs aan de persoon, 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 activiteiten of voorzieningen 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

Bij het genereren van een coronatoegangsbewijs wordt een set identificerende gegevens (eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand) toegevoegd aan het coronatoegangsbewijs. 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 coronatoegangsbewijs 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 personen. 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.

18. Wat gebeurt er bij 'omzetting' van testuitslag naar coronatoegangsbewijs, hoe werkt de cryptografie?

Nadat een persoon een test op COVID-19 heeft gedaan bij een testuitvoerder, kan de ondertekende testuitslag worden opgehaald en in CoronaCheck of via coronacheck.nl worden geladen. Deze testuitslag is ondertekend met een private tekensleutel van de testuitvoerder.

Voor het ondertekenen van de testuitslag 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 coronatoegangsbewijs 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 CoronaCheck zien dat de gerandomiseerde handtekening geldig blijft.

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

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

De controleur scant het coronatoegangsbewijs (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 CoronaCheck Scanner 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 coronatoegangsbewijs (groen scherm in CoronaCheck Scanner), of ‘geen geldig coronatoegangsbewijs’ (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 COVID-19 heeft. De controleur kan de persoon niet herkennen aan de uniekheid van de handtekening, omdat deze steeds gerandomiseerd wordt.

20. 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 coronatoegangsbewijs.
- In CoronaCheck 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 de persoon.

21. Hoe wordt de communicatie van en naar CoronaCheck beveiligd

CoronaCheck en coronacheck.nl (bij het genereren van een coronatoegangsbewijs 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 CoronaCheck 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 CoronaCheck 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 CoronaCheck, alsmede voor de uitslag berichten van commerciële partijen. Deze laatsten dienen op een expliciete lijst te staan alvorens geaccepteerd te worden.