# Gegevensbeschermingseffectbeoordeling (DPIA)

**VWS | Directie Informatiebeleid / CIO**

**DPIA EU Digitaal Corona Certificaat & nationaal Coronatoegangsbewijs**

Den Haag, 21 juni 2021 / versie 2.0 / Status: vastgesteld

Vaststelling verwerkingsverantwoordelijke:
Functie: Directeur Programmadirectie Covid-19

Kennisgenomen van FG-advies
Acceptatie restrisico na genomen maatregelen

Datum akkoord: 21 juni 2021

Advies Functionaris voor Gegevensbescherming VWS: 16 juni 2021

# Gegevensbeschermingseffectbeoordeling (DPIA)

**VWS | Directie Informatiebeleid / CIO**

**DPIA EU Digitaal Corona Certificaat (DCC) & nationaal Coronatoegangsbewijs**

**Contact:**

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

Versie: 2.0, 21 juni 2021

# Inhoudsopgave

# Inleiding

**Aanleiding**
Deze gegevensbeschermingseffectbeoordeling (hierna: DPIA) is opgesteld door het programma 'Realisatie Digitale Ondersteuning' binnen het Ministerie van Volksgezondheid, Welzijn en Sport (hierna: VWS) en geldt voor het EU Digitaal Corona Certificaat (hierna: EU DCC) en het Coronatoegangsbewijs voor nationaal gebruik. Deze DPIA vervangt de DPIA CoronaCheck en Coronatoegangsbewijs, versie 1.4 .

**EU Digitaal Corona Certificaat**
Op 14 juni 2021 is de Verordening (EU) 2021/953 van het Europees Parlement en de Raad betreffende een kader voor de afgifte, verificatie en aanvaarding van interoperabele COVID-19-vaccinatie-, test- en herstelcertificaten (digitaal EU-COVID-certificaat) teneinde het vrije verkeer tijdens de COVID-19-pandemie te faciliteren, gepubliceerd (hierna: de verordening). De verordening ziet op een Europees (technisch) kader voor de uitgifte van interoperabele certificaten inzake COVID-19-vaccinatie, -testen en –herstelbewijzen met als doel om het vrij verkeer van personen te bevorderen (artikel 21 VWEU). De certificaten moeten zowel digitaal als in papieren vorm kunnen worden afgegeven. De verordening schrijft bovendien het opstellen en onderhouden van een door de Commissie en lidstaten gebouwd trust framework voor, een infrastructuur waarmee de authenticiteit van een certificaat kan worden geverifieerd.

De verordening heeft rechtstreekse werking en bevat tevens wettelijke grondslagen voor het verwerken van gegevens voor het uitgeven en verifiëren van de EU DCC als het gaat om het bevorderen van vrij verkeer van personen. Het verplicht lidstaten tot de uitgifte van vaccinatie-, test- en herstelbewijzen. De verordening treedt op 1 juli 2021 in werking en biedt lidstaten zes weken de tijd om het uitgeven van de certificaten volgens de in de verordening afgesproken voorwaarden in te regelen. De verordening kent een werkingsduur van 12 maanden en kan eventueel verlengd worden in het kader van COVID-19.

Vanwege het non-discriminatiebeginsel, zoals neergelegd in art. 18 VWEU, zal gelijke behandeling gelden van alle Europese burgers. Dit betekent dat als in Nederland besloten wordt dat op basis van een nationaal vaccinatie-, test- of herstelbewijs, toegang verleend kan worden aan een evenement of locatie, dit niet alleen zal gelden voor Nederlandse burgers, maar ook voor Europese burgers met een EU DCC indien wordt voldaan aan de eisen met betrekking tot toegang die in Nederland worden gesteld.

**Nationaal Coronatoegangsbewijs**
De Tijdelijke wet coronatoegangsbewijzen regelt de tijdelijke inzet van een toegangsbewijs op basis van een negatieve testuitslag omtrent infectie met dat virus, een bewijs van vaccinatie tegen dat virus en herstel van een infectie met dat virus. Dit om te kunnen bijdragen aan het verantwoord openen of geopend houden van onderdelen van de samenleving bij de bestrijding van de epidemie van Covid-19. De Tijdelijke wet coronatoegangsbewijzen is op 1 juni 2021 in werking getreden.

**CoronaCheck, coronacheck.nl, CoronaCheck Scanner en hulpverlenersportaal (HKVI) voor zowel EU DCC als Coronatoegangsbewijs**

De CoronaCheck app wordt reeds ingezet voor het genereren van een digitaal Coronatoegangsbewijs (in de vorm van een QR-code) op basis van een negatieve testuitslag. Daarnaast kan een persoon kiezen om een Coronatoegangsbewijs te genereren dat geschikt is om te printen via coronacheck.nl. Dit wordt voor binnenlands gebruik stapsgewijs uitgebreid met een Coronatoegangsbewijs op basis van vaccinatiegegevens (vaccinatiebewijs) en een positief testresultaat (herstelbewijs). Vanaf 1 juli 2021 wordt het tevens mogelijk om via CoronaCheck of coronacheck.nl het EU DCC ten behoeve van reizen (de Europese QR-code) te gebruiken (voor vaccinatie, herstel of negatieve test). Via dezelfde applicatie en website kan dus zowel een nationaal Coronatoegangsbewijs als een EU DCC worden gegenereerd.

Voor binnenlands gebruik wordt voor het uitlezen van de QR-code door de controleurs gebruik gemaakt van de CoronaCheck Scanner om te controleren of iemand beschikt over een geldig Coronatoegangsbewijs. Deze zal tevens worden ingezet voor de controle van een EU DCC van een Europese burger uit een andere lidstaat die toegang wil tot een evenement of locatie in Nederland. Nederland heeft ervoor gekozen om de EU DCC niet in te zetten voor binnenlands gebruik door Nederlandse burgers aangezien de EU DCC meer gegevens bevat dan noodzakelijk voor binnenlands gebruik. Het Nederlandse Coronatoegangsbewijs is zo ontworpen dat de QR-code minimale data bevat en de controleur niet kan zien of iemand beschikt over een vaccinatie-, test- of herstelbewijs. De eisen die gelden voor de gegevens die zijn opgenomen in de QR-code van het EU DCC ten behoeve van reizen zijn uitgebreider en bevatten meer persoonsgegevens.

Indien het een persoon niet lukt via CoronaCheck of coronacheck.nl een EU DCC en een Coronatoegangsbewijs te genereren, is voorzien in een hulpverlenersportaal (HKVI).

Verder is, als het gaat om uitreizen, de minister van Infrastructuur en Waterstaat ervoor verantwoordelijk dat de invoering van het EU DCC in het georganiseerde vervoer goed verloopt. De minister van Justitie en Veiligheid heeft de verantwoordelijkheid voor de controle en handhaving van inreizigers met eigen vervoer.

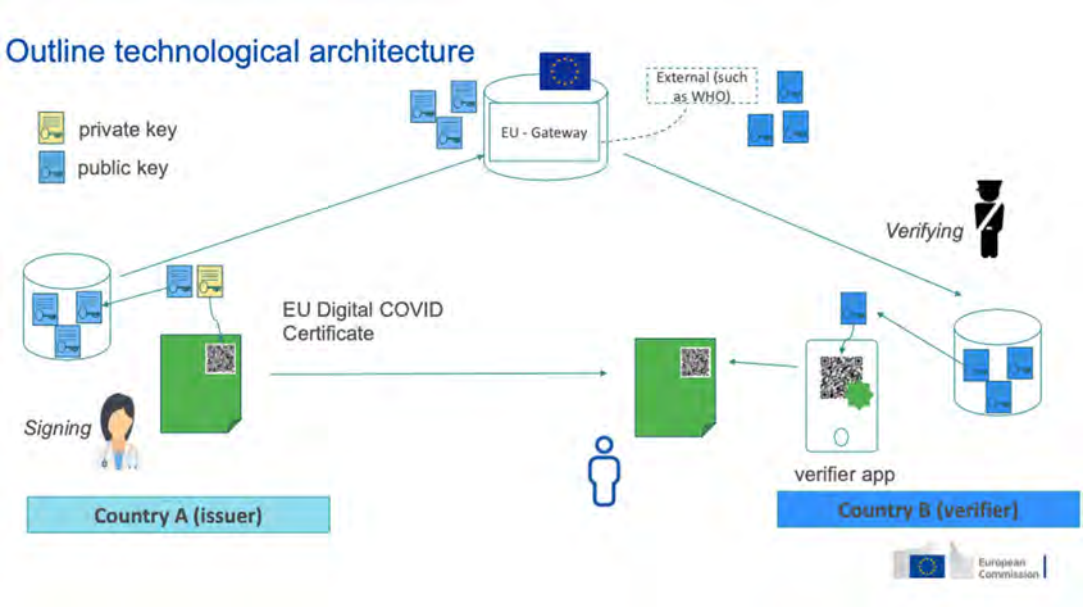
De applicaties CoronaCheck, CoronaCheck Scanner, de websitecoronacheck.nl en het hulpverlenersportaal (HKVI) zijn onder verantwoordelijkheid van de minister van VWS (hierna de minister) ontwikkeld. Het uitgangspunt van deze DPIA is het voorgenomen gebruik van(persoons)gegevens zoals bekend op 21 juni 2021.

**Reikwijdte DPIA**

Deze DPIA geldt voor het EU DCC ten behoeve van reizen en voor het Coronatoegangsbewijs voor nationaal gebruik.

De verordening treedt 1 juli 2021 in werking. Door middel van een EU DCC kan het vrij verkeer van personen op een veilige wijze worden gefaciliteerd gedurende de pandemie en wordt voorkomen

dat elke lidstaat een eigen oplossing kiest die niet interoperabel is. Door middel van een *trust framework* kan de authenticiteit van een certificaat van een lidstaat in een andere lidstaat worden geverifieerd Dit gehele proces ziet er op het niveau van de EU als volgt uit:




Deze DPIA ziet op het deel van bovenstaand proces dat onder verantwoordelijkheid valt van de minister van VWS als het gaat om de uitgifte van het certificaat (Country A). Voor zover dit noodzakelijk is voor de duidelijkheid en leesbaarheid worden onderdelen die buiten scope vallen meegenomen in de beschrijving. Dit wordt aangegeven in de tekst.

Daarnaast ziet deze DPIA op het proces van uitgifte van een Coronatoegangsbewijs ten behoeve van binnenlands gebruik en het uitlezen daarvan door middel van een door de minister van VWS uitgegeven CoronaCheck Scanner.

<u>Binnen de reikwijdte van deze DPIA valt:</u>

- Het gehele proces van de uitgifte van een EU DCC en een Coronatoegangsbewijs aan de Nederlandse burger.
    - Voor zowel test-, vaccinatie-, als herstel.
    - Voor zowel de digitale route (via CoronaCheck) als de papieren route (printen via coronacheck.nl).
    - Voor de route via het hulpverlenersportaal, dit indien het de persoon niet lukt via CoronaCheck of coronacheck.nl een EU DCC of een Coronatoegangsbewijs te genereren.
    - De benodigde koppelvlakken met de bronsystemen die de gegevens moeten leveren voor het uitgeven van een EU DCC en een Coronatoegangsbewijs, met inbegrip van de technische specificatie van deze koppelvlakken.
    - De benodigde koppeling met de infrastructuur van de Commissie (trust framework) in het geval van een EU DCC.

- Het gebruik van de CoronaCheck Scanner als het gaat om het uitlezen van een Coronatoegangsbewijs om toegang te verkrijgen tot een evenement of locatie in Nederland waarvoor geldt dat toegang kan worden verkregen op basis van de Tijdelijke wet coronatoegangsbewijzen.
- Het gebruik van de CoronaCheck Scanner als het gaat om het uitlezen van de EU DCC van personen uit andere lidstaten die toegang willen tot een evenement of locatie in Nederland waarvoor geldt dat toegang kan worden verkregen op basis van een nationaal coronatoegangsbewijs.

<u>Buiten reikwijdte van deze DPIA valt:</u>

- De gegevensverwerking bij de uitvoerders van de test, de vaccinatiezetter en de verklaarder van herstel.
- De Scan app voor het uitlezen van het EU DCC in het kader van georganiseerd vervoer en controle van inreizigers met eigen vervoer.
- De Scan app voor het uitlezen van het EU DCC door een andere lidstaat.
- Het *trust framework* en de daarmee samenhangende Europese spelregels over welke vaccins en tests erkend worden en de te hanteren beslisregels over hoe lang welke test of vaccin een significante verlaging van het besmettingsgevaar van de betrokkene met zich meebrengt.
- De uitzonderingsroutes die momenteel nog worden ontwikkeld, bijvoorbeeld voor mensen die niet beschikken over een BSN.
- De wijze waarop voor de inwoners van de BES-eilanden zal worden voorzien in de uitgifte van een EU DCC.
- De wijze waarop zal worden geregeld dat de CAS-landen kunnen aansluiten op het systeem dat de EU bouwt om vaccinatie-, test en herstelbewijzen te authentiseren en verifiëren.
- Het publiceren van de app in de relevante app stores is in zoverre binnen de reikwijdte van deze DPIA dat risico's op "valse" apps onderdeel uit zullen maken van de risico-analyse. Eventuele verwerkingen in deze app stores van persoonsgegevens door Apple en/of Google vallen buiten de reikwijdte van deze DPIA.
- Het broncodedepot van de CoronaCheck app.
- Het inloggen door de persoon in de CoronaCheck app vindt plaats met DigiD via de ToegangVerleningService (TVS). Beide worden beschouwd als een bouwsteen waarvan het gebruik wel binnen de reikwijdte van deze DPIA valt maar niet de werking. Beide bouwstenen vallen onder de verantwoordelijkheid van de minister van BZK.

**Gebruikte afkortingen en definities**

| | |
|---|---|
| AVG | Algemene verordening gegevensbescherming |
| Betrokkene | Geïdentificeerde of identificeerbare natuurlijke persoon: als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatie-nummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (vgl. artikel 4, onder 1) van de AVG) |
| Bewijsmiddel | Digitaal gewaarmerkt test-, vaccinatie of herstelbewijs, ongedifferentieerd voor EU of Nederlands gebruik. |
| Coronatoegangsbewijs | Een bewijsmiddel dat betrokkene een beperkt COVID-19 besmettingsgevaar vormt voor binnenlands gebruik dat op een test-, vaccinatie- of herstelverklaring gebaseerd kan zijn. |
| BRP | Basisregistratie Personen |
| BSN | Burgerservicenummer |
| BZK | Ministerie van Binnenlandse Zaken en Koninkrijksrelaties |
| Controleur | Iemand die de geldigheid van een Coronatoegangsbewijs of EU DCC van een burger uit een andere lidstaat controleert |
| DICTU | Dienst ICT Uitvoering |
| eIDAS | Electronic IDentification, Authentication and trust Services, Verordening 910/2014/EU. |
| EU DCC | EU Digitaal Corona Certificaat: een interoperabel certificaat met informatie over de vaccinatie-, test- en/of herstelstatus van de houder, afgegeven in de context van de COVID-19-pandemie.[1] |
| EER | Europese Economische Ruimte |

[1] Vgl. artikel 2 (2) van de Verordening van het Europees Parlement en de Raad betreffende een kader voor de afgifte, verificatie en aanvaarding van interoperabele vaccinatie-, test-, en herstelcertificaten teneinde het vrije verkeer tijdens de COVID-19-pandemie te vergemakkelijken.

| | |
|---|---|
| IenW | Ministerie van Infrastructuur en Waterstaat |
| Minister van VWS | Minister van Volksgezondheid, Welzijn en Sport |
| NAAT | Nucleic Acid Amplification Test, een test voor DNA-markeringen in een monster |
| PCR-test | Polymerase Chain Reaction-test, een specifiek type NAAT |
| TVS | ToegangVerleningService |

# A. Beschrijving kenmerken gegevensverwerking

**Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.**

## 1. Voorstel

### 1.1 Uitgifte Bewijsmiddel

Een Bewijsmiddel (EU DCC of Coronatoegangsbewijs) is een digitaal gewaarmerkt bewijs van vaccinatie tegen COVID-19 (vaccinatiebewijs), negatieve COVID-19-test (testbewijs) of herstel van COVID-19 (herstelbewijs) met een bijbehorende QR-code. Dit voorstel ziet op de *twee hoofdroutes* die een persoon kan volgen om een Bewijsmiddel te genereren.

1. **App**: Route Digitaal Bewijsmiddel (via de CoronaCheck app)
2. **Website**: Route website Bewijsmiddel (via de website https://coronacheck.nl)

Deze routes zijn zowel van toepassing op het genereren van een EU DCC als een Coronatoegangsbewijs op basis van test-, vaccinatie- en herstelgegevens.

**Terminologie:**

**Omdat het de leesbaarheid niet ten goede komt als we telkens test-, vaccinatie- of herstelbewijs schrijven (al dan niet in de nationale of EU variant) gebruiken we de volgende termen:**

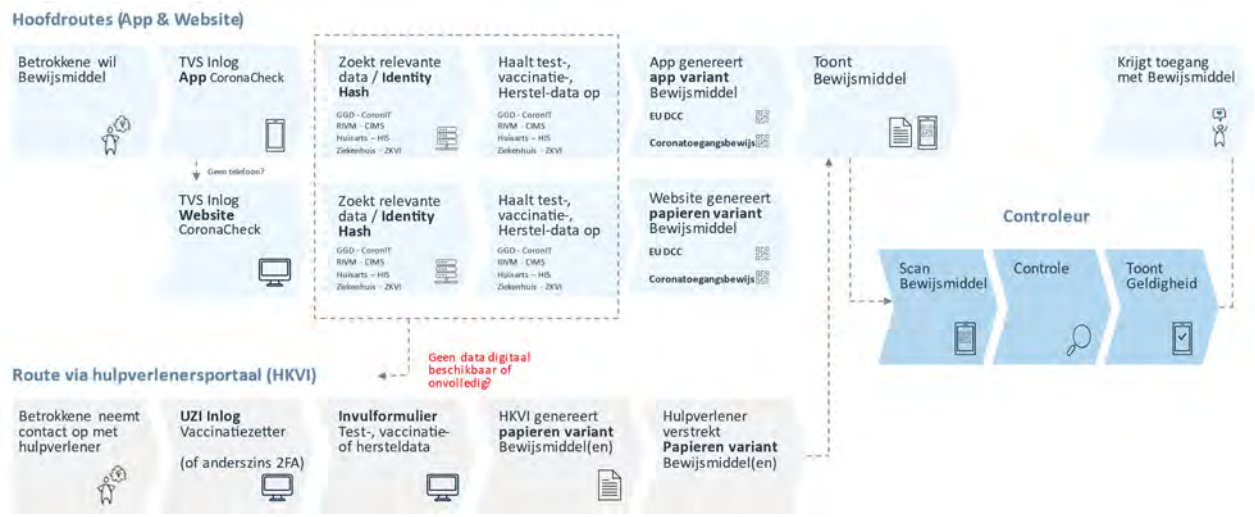
- **Bewijsmiddel: digitaal gewaarmerkt test,- vaccinatie- of herstelbewijs, ongedifferentieerd voor EU of Nederlands gebruik;**
- **EU DCC: een Europees Bewijsmiddel;**
- **Coronatoegangsbewijs: het Nederlandse Bewijsmiddel voor binnenlands gebruik.**

**Daar waar specifiek verwezen wordt naar een Bewijsmiddel op basis van een negatieve test, vaccinatie of verklaring zal in dit document de term test-, vaccinatie- of herstelbewijs worden gebruikt.**

Daarnaast ziet dit voorstel op een derde route:

- de route via het **Hulpverlenersportaal (HKVI)**. Hierbij kan een persoon contact opnemen met de hulpverlener die de vaccinatie heeft gezet of de test heeft uitgevoerd. De hulpverlener voert dan via een speciaal daarvoor door VWS ontwikkeld portaal de gegevens van de persoon in en genereert via hetzelfde proces als bij route via de app en de website een bewijsmiddel op papier. Deze kan vervolgens worden opgestuurd aan de persoon of deze kan het bewijsmiddel komen ophalen.

Deze derde route is om meerdere redenen van belang, met name voor kwetsbare groepen zoals personen die geen toegang hebben tot een smartphone, pc of printer óf niet in staat zijn via de app of website een bewijsmiddel te genereren. Daarnaast kan deze route een oplossing bieden voor situaties waarin de app of de website geen gegevens vinden maar een persoon wél is gevaccineerd of getest. De verordening verplicht lidstaten – juist om uitsluiting van kwetsbare groepen te voorkomen - ervoor te zorgen dat aan wie dit wil (zie overweging 18 van de verordening) een EU DCC op papier wordt verstrekt bijvoorbeeld via de post of dat het opgehaald kan worden bij een afhaalpunt.




*Figuur 1 Routes Bewijsmiddelen (vereenvoudigd)*

Deze drie routes zijn zowel van toepassing op het genereren van een EU DCC en Coronatoegangsbewijs op basis van test-, vaccinatie- als herstelgegevens.
Momenteel wordt onderzocht of er nog meer situaties zijn die een aparte uitzonderingsroute vereisen, deze vallen buiten scope van deze DPIA. Deze uitzonderingsroutes zullen in de vorm van een addendum bij deze DPIA worden gevoegd.

De twee hoofdroutes én de route via het Hulpverlenersportaal worden onderstaand op hoofdlijnen beschreven. In paragraaf 3 wordt dit voor testen, vaccinatie en herstel apart nader uitgewerkt.

### *App: Route Digitaal Bewijsmiddel via CoronaCheck App*

1. Betrokkene downloadt de CoronaCheck app in een appstore (doorgaans Apple App Store of Google Play Store) en installeert deze.
2. De CoronaCheck app zal met behulp van een configuratieserver van VWS (hierover later meer) een aantal instellingen ophalen.
3. In de CoronaCheck app wordt bij eerste gebruik in een onboardingsproces aan de betrokkene uitgelegd wat de Bewijsmiddelen in kunnen houden en waar ze voor gebruikt kunnen worden. Daarbij wordt de betrokkene in de gelegenheid gesteld de privacyverklaring te lezen.


4. Betrokkene geeft in de CoronaCheck app aan dat hij een test-, vaccinatie- of herstelbewijs wenst aan te maken.
5. De identiteit van de betrokken wordt geverifieerd (hetzij door DigiD-niveau midden, hetzij door middel van een door een privaat teststation uitgereikte unieke ophaalcode en verificatiecode[2], beide twee-factor authenticatie).
6. Als de betrokkene in stap 4 heeft aangegeven alleen een testbewijs te willen ophalen worden de gegevens bij het teststation of bij de GGD'en opgehaald en vervolgt het proces met stap 8. Als betrokkene in stap 4 heeft aangegeven een andersoortig Bewijsmiddel (dus vaccinatie- of herstelbewijs) te willen volgt stap 7.
7. De benodigde gegevens worden bij de bronhouders (RIVM, vaccinatiezetter of verklaarder van herstel) opgevraagd.
8. Betrokkene bevestigt dat hij op basis van de beschikbare informatie een QR-code wil maken.
9. De opgehaalde informatie wordt beoordeeld aan de hand van de vereisten die op Europees niveau worden gesteld voor het verkrijgen van een EU DCC én aan de hand van de vereisten die op nationaal niveau worden gesteld voor het verkrijgen van een Coronatoegangsbewijs.
10. Indien de opgehaalde informatie voldoet aan de hiervoor genoemde vereisten, worden de beide Bewijsmiddelen (EU DCC / Coronatoegangsbewijs) door VWS verstrekt en in de CoronaCheck app opgeslagen. In het geval van het EU DCC is dat een QR-code, in het geval van het Coronatoegangsbewijs is dat een dataset die voorzien is van een gekwalificeerde elektronische handtekening op basis waarvan QR-codes die deze informatie bevatten gegenereerd kunnen worden. Het technische verschil tussen het EU DCC en het Coronatoegangsbewijs is, ook al worden ze beide als QR-codes getoond, a) dat ze andere gegevens bevatten en b) met technisch andere gekwalificeerde elektronische handtekeningen ondertekend zijn. Daarom worden hier twee verschillende signing servers van VWS voor gebruikt. Praktisch gezien wordt voor een periode van maximaal 28 dagen (minder in het geval van een testbewijs) een set QR-codes verstrekt (een strippenkaart) die het mogelijk maakt eens per 90 seconden een andere QR-code te tonen die ondertekend is door de minister van VWS.
11. De toegekende Bewijsmiddelen worden in de CoronaCheck app opgeslagen, samen met de bij stap 6 of 7 opgehaalde gegevens (met ondertekeningen van de bronhouders) zodat deze later opnieuw aangeboden kunnen worden aan de signing servers ter ondertekening voor een nieuwe periode van 28 dagen.

[2] De wijze waarop wordt voor de commerciële teststations aan de teststations gehouden, in de aansluitvoorwaarden wordt twee-factor authenticatie vereist.

*Website: Route Fysiek Bewijsmiddel via Website https://coronacheck.nl*

1. Betrokkene geeft op de Website aan dat hij of zij zijn of een test-, vaccinatie- of herstelbewijs wenst.
2. De identiteit van de betrokken wordt geverifieerd (hetzij door DigiD-niveau midden, hetzij door middel van een door een privaat teststation uitgereikte unieke ophaalcode en verificatiecode, beide twee-factor authenticatie)[3].
3. Als de betrokkene in stap 1 heeft aangegeven alleen een testbewijs te willen ophalen worden de gegevens bij het teststation of bij de GGD'en opgehaald en vervolgt het proces met stap 5. Als betrokkene in stap 1 heeft aangegeven een andersoortig Bewijsmiddel te willen volgt stap 4.
4. De benodigde gegevens worden bij de bronhouders (vaccinatiezetter of verklaarder van herstel) opgevraagd.
5. Betrokkene bevestigt dat hij op basis van de beschikbare informatie een QR-code wil maken.
6. De opgehaalde informatie wordt beoordeeld aan de hand van de vereisten die op Europees niveau worden gesteld voor het verkrijgen van een EU DCC én aan de hand van de vereisten die op nationaal niveau worden gesteld voor het verkrijgen van een Coronatoegangsbewijs.
7. Indien de opgehaalde informatie voldoet aan de hiervoor genoemde vereisten, worden de beide Bewijsmiddelen (EU DCC / Coronatoegangsbewijs) door VWS verstrekt. De Bewijsmiddelen worden in de vorm van QR-codes getoond en ter download aangeboden in PDF-formaat. Het technische verschil tussen het EU DCC en het Coronatoegangsbewijs is, ook al worden ze beide als QR-codes getoond, a) dat ze andere gegevens bevatten en b) met technisch andere gekwalificeerde elektronische handtekeningen ondertekend zijn. Daarom worden hier twee verschillende signing servers van VWS voor gebruikt.
8. Betrokkene kan de Bewijsmiddelen in de vorm van een QR-code in PDF-bestanden downloaden en op papier printen en beschikt daarmee over een EU DCC en Coronatoegangsbewijs op papier.

*HKVI: Route Fysiek Bewijsmiddel via hulpverlenersportaal*

1. Betrokkene wendt zich tot de vaccinatiezetter of de uitvoerder van de test met het verzoek om een Bewijsmiddel te genereren;
2. De vaccinatiezetter of de uitvoerder van de test logt in op het HKVI met:
   a) UZI-pas, of
   b) Twee-factor-authenticatie (indien vooraf hiervoor aangemeld door de verantwoordelijke arts en gecontroleerd[4])
3. De vaccinatiezetter of uitvoerder van de test vult de benodigde informatie voor een Bewijsmiddel in;
4. De vaccinatiezetter of uitvoerder van de test bevestigt dat het Bewijsmiddel gegenereerd moet worden;

[3] De wijze waarop wordt voor de commerciële teststations aan de teststations gehouden, in de aansluitvoorwaarden wordt twee-factor authenticatie vereist.

[4] Niet alle artsen (of hun gedelegeerden) hebben de beschikking over een UZI-pas.

5. De door de vaccinatiezetter of uitvoerder van de test verstrekte informatie wordt beoordeeld aan de hand van de vereisten die op Europees niveau worden gesteld voor het verkrijgen van een EU DCC én aan de hand van de vereisten die op nationaal niveau worden gesteld voor het verkrijgen van een Coronatoegangsbewijs.
6. Indien de door de vaccinatiezetter of uitvoerder van de test verstrekte informatie voldoet aan de hiervoor genoemde vereisten, worden de Bewijsmiddelen (zowel EU DCC als Coronatoegangsbewijs) door VWS verstrekt. De Bewijsmiddelen worden in de vorm van QR-codes getoond. Het technische verschil tussen het EU DCC en het Coronatoegangsbewijs is, ook al worden ze beide als QR-codes getoond, a) dat ze andere gegevens bevatten en b) met technisch andere gekwalificeerde elektronische handtekeningen ondertekend zijn. Daarom worden hier twee verschillende signing servers van VWS voor gebruikt.
7. De vaccinatiezetter of de uitvoerder van de test kan de Bewijsmiddelen in de vorm van QR-codes in PDF-bestanden downloaden en op papier printen. Vervolgens kunnen de bewijsmiddelen naar de betrokkene worden verstuurd of deze kan ze komen ophalen.

## 1.2 CoronaCheck Scanner: uitlezen EU DCC van burger uit andere lidstaat

### *CoronaCheck Scanner: uitlezen EU DCC van personen uit andere lidstaten voor toegang evenementen en locaties in Nederland*

De CoronaCheck Scanner die door VWS is ontwikkeld is primair bedoeld voor het scannen van binnenlandse coronatoegangsbewijzen, maar zal ook EU DCC's uit kunnen lezen die buiten Nederland zijn uitgegeven aan burgers van een andere EU-lidstaat. Vanwege het non-discriminatiebeginsel, zoals neergelegd in art. 18 VWEU, zal gelijke behandeling gelden van alle Europese burgers. Dit betekent dat als in Nederland besloten wordt dat op basis van een Coronatoegangsbewijs, toegang verleend kan worden aan een evenement of locatie, dit niet alleen zal gelden voor Nederlandse burgers, maar ook voor Europese burgers met een EU DCC indien geldig voor Nederland.
De CoronaCheck Scanner is zo gebouwd dat ook bij het uitlezen van de QR-code van een EU DCC door de controleur, die meer gegevens bevat dan de QR-code voor nationaal gebruik, toch alleen de gegevens worden getoond die te zien zijn bij het uitlezen van een nationaal Coronatoegangsbewijs. De CoronaCheck Scanner toont "rood" of "groen" en bij een groen scherm vervolgens de eerste letter voornaam, eerste letter achternaam, geboortemaand en geboortedag, zodat geverifieerd kan worden dat de toonder van de EU DCC dezelfde persoon is als degene aan wie het uitgereikt is.

### *Scanner app voor uitreizen en inreizen*

Als het gaat om uitreizen is de minister van Infrastructuur en Waterstaat ervoor verantwoordelijk dat de invoering van het EU DCC in het georganiseerde vervoer goed verloopt. De minister van Justitie en Veiligheid heeft de verantwoordelijkheid voor de controle en handhaving van inreizigers met eigen vervoer. De Scan app die hiervoor zal worden ingezet valt daarmee niet binnen scope van deze DPIA. Dit geldt ook voor de Scan apps die door de andere lidstaten worden gebruikt voor het uitlezen van de EU DCC van personen die naar hun land reizen. Wel is in paragraaf 2 nader

uitgewerkt welke gegevens zijn opgenomen in de QR-code van het EU DCC die door genoemde partijen kunnen worden uitgelezen.

Uit hoofde van zowel betrouwbaarheid als privacy wordt vanuit de Verordening de eis gesteld (overweging 22 van de verordening) dat de verificatie van het EU DCC offline plaats kan vinden zodat de lidstaat die het EU DCC heeft uitgegeven of een andere partij geen informatie krijgt over waar en wanneer de verificatie plaatsvindt. Dit wordt gerealiseerd door periodiek de publieke sleutels van de uitgevende lidstaten in de CoronaCheck Scanner in te laden. Dit sleutelbeheer vindt plaats op basis van het European trust framework dat dit mogelijk maakt (zie paragraaf 8 voor nadere uitwerking). **Verificatie door middel van de VWS CoronaCheck Scanner leidt niet tot netwerkverkeer met het land van uitgifte. Hiermee wordt voorkomen dat het land van uitgifte door dergelijk netwerkverkeer haar onderdanen zou kunnen volgen.**

### 1.3 Corona Scan App: uitlezen Coronatoegangsbewijs uit CoronaCheck app

Zoals eerder aangegeven is het Coronatoegangsbewijs intern in de CoronaCheck app nog geen QR-code, maar een van een gekwalificeerde elektronische handtekening voorziene dataset voor het Coronatoegangsbewijs. Deze dataset heeft een afgiftedatum en een geldigheidsduur.

De CoronaCheck app genereert op basis hiervan QR-codes die iedere 90 seconden veranderen in de app. In deze veranderende QR-code zelf staat een afgiftetijdstip en een geldigheidsduur van 24 uur. Omdat in het geval het Coronatoegangsbewijs gebaseerd is op een testbewijs het einde van de laatste 24 uurstermijn voorbij de geldigheidsduur van het testbewijs kan vallen wordt het afgiftetijdstip zo nodig geantedateerd.

**Hiermee wordt het Coronatoegangsbewijs een soort strippenkaart die het volgen van gebruikers van het Coronatoegangsbewijs bemoeilijkt én waardoor niet valt af te leiden of het Coronatoegangsbewijs is gebaseerd op een test-, vaccinatie- of herstelbewijs. Een strip is immers nooit langer dan één dag geldig.**

Deze 24-uurs-QR-code kan getoond worden aan een gebruiker van de CoronaCheck Scanner. Deze toont “rood” of “groen” en bij een groen scherm de volgende set gegevens: eerste letter voornaam, eerste letter achternaam, geboortemaand en geboortedag van de betrokkene, zodat geverifieerd kan worden dat de toonder van het Coronatoegangsbewijs dezelfde persoon is als degene aan wie het uitgereikt is. Deze set aan identificerende gegevens kan bij een digitaal coronatoegangsbewijs nog beperkt worden om de mogelijkheid tot herleidbaarheid van de persoon te verminderen.

### 1.4 Corona Scan App: uitlezen papieren Coronatoegangsbewijs

Het “papieren” Coronatoegangsbewijs zoals verkregen via de Website of via het hulpverlenersportaal (HKVI) kan getoond worden aan een gebruiker van de CoronaCheck Scanner. De CoronaCheck Scanner toont “rood” of “groen” en bij een groen scherm vervolgens de eerste letter voornaam, eerste letter achternaam, geboortemaand en geboortedag, zodat geverifieerd kan worden dat de toonder van het Coronatoegangsbewijs dezelfde persoon is als degene aan wie het uitgereikt is. Bij een papieren Coronatoegangsbewijs worden alle bovenstaande gegevens getoond.

Opgemerkt moet worden dat de QR-code van het papieren Coronatoegangsbewijs, omdat dit niet tussentijds kan veranderen, een vaste geldigheidsduur heeft.

## 2. Persoonsgegevens

Onderstaand worden alle persoonsgegevens opgesomd die worden verwerkt en wordt tevens aangegeven welke categorieën van persoonsgegevens het betreft. Een onderscheid wordt gemaakt in de persoonsgegevens die verwerkt worden om de Bewijsmiddelen af te geven (2.1) en de persoonsgegevens die vervolgens zijn opgeslagen in de relevante QR-code(s) (2.2).

### 2.1 Persoonsgegevens die worden verwerkt bij uitgifte Bewijsmiddelen

*Gegevens die worden verwerkt voor de uitgifte van een Bewijsmiddel (test, vaccinatie en herstel). Dit geldt dus zowel voor het genereren van een EU DCC als een Coronatoegangsbewijs.*

- IP-adres wat betrokkene gebruikt bij het aan laten maken van het Bewijsmiddel
- BSN van betrokkene
- Voor- en achternamen van betrokkene
- Organisatie bij wie vaccinatie-, of herstelgegevens zijn opgehaald.
    - Bij test- of herstelbewijs:
        - unieke code van de test
        - type test
        - testnaam
        - datum en tijd testafname
        - datum en tijd van vaststelling testresultaat
        - ziekteverwekker waar voor getest is
        - testproducent
        - naam van testcentrum
        - uitslag van de test (negatief voor testbewijs, positief voor herstelbewijs)
    - Alleen bij vaccinatiebewijs:
        - datum toediening
        - unieke code van vaccinatie
        - ziekteverwekker waar het vaccin tegen werkt
        - vaccintype
        - vaccinnaam
        - handelsvergunninghouder of producent van het vaccin
        - volgnummer in reeks vaccinaties/doses
- Alleen bij HKVI: IP-adres en inloggegevens van de hulpverlener (UZI-pas of diens accountgegevens).

### 2.2 Persoonsgegevens die zijn opgeslagen in het Bewijsmiddel (QR-code)

**Coronatoegangsbewijs**

*De QR-code voor het Coronatoegangsbewijs wordt elke 90 seconden (enkel in de app) opnieuw gegenereerd en bevat:*

- Startdatum en einddatum geldigheid Coronatoegangsbewijs
- Eerste letter voornaam, eerste letter achternaam
- Geboortemaand en geboortedag
- Indicatie of de code digitaal of als fysiek Bewijsmiddel is uitgegeven

Met dien verstande dat deze set aan identificerende gegevens bij een digitaal Coronatoegangsbewijs nog beperkt kan worden om de mogelijkheid tot herleidbaarheid van de persoon te verminderen.

**EU DCC**
*Persoonsgegevens die in de EU DCC (QR-code) zijn opgenomen ongeacht het type (test-, vaccinatie- of herstelbewijs):*

- Naam: familienaam of familienamen en voornaam of voornamen en eventueel tussenvoegsel
- Geboortedatum
- Doelziekte of ziekteverwekker (bijvoorbeeld: SARS-CoV-2 en/of varianten daarop)
- Unieke certificaatidentificatiecode
- Lidstaat waar test/vaccinatie is uitgevoerd of herstelbewijs is verkregen
- Afgever van het EU DCC, dat is voor Nederland de minister van VWS

*De QR-code voor het EU DCC als testbewijs bevat naast de algemene gegevens:*

- Geregistreerde datum en tijdstip van testafname
- Type test
- Naam van de test(facultatief voor NAAT (PCR) test)
- Naam van de testproducent (facultatief voor NAAT (PCR) test)
- Testresultaat
- Testcentrum of – faciliteit (optioneel bij snelle antigeentest)

*De QR-code voor het EU DCC als vaccinatiebewijs naast de algemene gegevens:*

- Vaccin/profylaxe (type vaccin, bv. mRNA-vaccin of antigen-vaccin)
- Vaccin-naam
- Handelsvergunninghouder of producent van het vaccin
- Volgnummer in reeks vaccinaties/doses
- Vaccinatiedatum, met vermelding datum van laatst ontvangen dosis

*De QR-code voor het EU DCC als herstelbewijs bevat in aanvulling op de algemene gegevens de volgende gegevens:*

- Datum eerste positieve testresultaat (NAAT)
- Datum vanaf wanneer certificaat geldig is
- Datum tot wanneer certificaat geldig is

## 2.3 Persoonsgegevens die worden verwerkt bij het uitlezen door de CoronaCheck Scanner

Afhankelijk van het Bewijsmiddel (EU DCC of Coronatoegangsbewijs) worden er verschillende persoonsgegevens verwerkt in de CoronaCheck Scanner. In het geval van het EU DCC zullen dat alle

gegevens zijn die in de QR-code van het EU DCC staan (zie paragraaf 2.1). In het geval van het Coronatoegangsbewijs is er voor gekozen minder gegevens in de QR-code op te nemen, dit zijn:

- Startdatum, -tijdstip en geldigheidsduur QR-code
- Eerste letter voornaam, eerste letter achternaam
- Geboortedag en geboortemaand

Voor alle Bewijsmiddelen geldt dat de CoronaCheck Scanner de volgende gegevens toont aan de controleur van een binnenlandse activiteit of evenement:

- Indicatie: 'Persoon beschikt over geldig Bewijsmiddel' (groen scherm) of 'Persoon beschikt niet over geldig Bewijsmiddel' (rood scherm).
- Een set identificerende gegevens: de eerste letter voornaam, eerste letter achternaam, geboortedag en -maand van betrokkene. Op basis van deze informatie in combinatie met het tonen van het identiteitsbewijs van betrokkene kan de controleur nagaan of het EU DCC of Coronatoegangsbewijs ook daadwerkelijk van betrokkene is. Zoals eerder aangegeven kan de set aan identificerende gegevens bij een digitaal Coronatoegangsbewijs beperkt worden om de mogelijkheid tot herleidbaarheid van de persoon te verminderen.

De genoemde gegevens verdwijnen van het scherm bij de eerstvolgende scan of anders uiterlijk na 240 seconden.[5]

## 2.4 Secundaire gegevens; verwerken IP-adres

Het omzetten van test-, vaccinatie-, of herstelgegevens in een door de minister van VWS digitaal ondertekend EU DCC of Coronatoegangsbewijs gaat via de signing servers van VWS (gehost door verwerker Prolocation). De gegevens worden hiervoor naar de webservers van VWS gestuurd die deze weer doorsturen naar de signing servers. Inherent aan internetcommunicatie is dat voor de communicatie met de webservers van VWS een IP-adres van de smartphone van de betrokkene wordt gebruikt. Het IP-adres wordt binnen de signing servers zelf niet vastgelegd, maar er vindt wel logging plaats door de webservers voor beveiligingsdoeleinden. In de context van de signing servers zijn IP-adressen 'gestript'[6] voordat deze bij een signing server komen, zodat desbetreffende signing server niet ziet welk bewijs aan welk IP-adres is gekoppeld. De signing servers "zien" dus geen externe IP-adressen, maar alleen het interne IP-adres van de webservers. De test-, vaccinatie- en herstelgegevens zelf zijn versleuteld, waardoor er compartimentering van informatie plaatsvindt. Vervolgens wordt de gekwalificeerde elektronische handtekening door de signing servers gezet en worden het EU DCC en het Coronatoegangsbewijs teruggestuurd naar de CoronaCheck app of https://coronacheck.nl. Op basis van deze informatie wordt een QR-code gegenereerd.

[5] 240 seconden is het maximum. Dit is geregeld in art. 6.32 van de tijdelijke regeling van de Ministers van Volksgezondheid, Welzijn en Sport, van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties tot wijziging van de Tijdelijke regeling maatregelen covid-19 in verband met de inzet van coronatoegangsbewijzen op basis van een negatieve testuitslag.

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

### 2.5 Categorisering persoonsgegevens

In bovenstaande tekst is opgesomd welke persoonsgegevens worden verwerkt. Het betreft gewone en bijzondere persoonsgegevens (namelijk: gezondheidsgegevens in de vorm van test-, vaccinatie- en herstelgegevens). Daarnaast worden wettelijk identificerende gegevens verwerkt (namelijk: het BSN van betrokkene). Er worden géén strafrechtelijke persoonsgegevens verwerkt.

## 3. Verwerkingen van persoonsgegevens

Onderstaand worden alle voorgenomen gegevensverwerkingen weergegeven.

### 3.1 Configuratie- en signing servers

Voor het beheer van de CoronaCheck app, coronacheck.nl, de CoronaCheck Scanner app en het hulpverlenersportaal is een configuratieserver actief. Bij het opstarten wordt informatie geconfigureerd. Deze configuratieserver bevat beslisregels zoals de duur van de geldigheid van test-, vaccinatie en herstelbewijzen en sleutels die gebruikt worden voor de beveiliging. Ook bevat de configuratieserver een mogelijkheid waarmee de service om test-, vaccinatie en herstelbewijzen te valideren tijdelijk of permanent beëindigd kan worden. Deze mogelijkheid kan worden gebruikt als de inzet van de CoronaCheck app, coronacheck.nl, de CoronaCheck Scanner en het hulpverlenersportaal definitief niet meer wenselijk wordt geacht.

Bij het ondertekenen wordt gebruik gemaakt van signing servers. Deze beoordeelt of de verzamelde of aangeleverde informatie (in het geval van HKVI) voldoende is om een Bewijsmiddel uit te geven. Verder ontdoen deze de verstrekte test-, vaccinatie- en herstelgegevens van de elektronische handtekeningen van de bronhouders/verstrekkers en in het geval van het Coronatoegangsbewijs ontdoet de specifieke signing server voor het Coronatoegangsbewijs dit van andere gegevens dan de initialen en de geboortedatum. Vervolgens ondertekenen de signing servers de uitslag namens de minister van VWS, maar alléén indien de opgehaalde informatie voldoet aan de vereisten die op Europees en nationaal niveau aan het EU DCC en Coronatoegangsbewijs worden gesteld.

### 3.2 Digitale route Bewijsmiddel op basis van testresultaat

*Test – Digitale route digitaal Bewijsmiddel via CoronaCheck App*

Deze paragraaf beschrijft het proces waarbij gebruik wordt gemaakt van de CoronaCheck app voor het genereren van een Bewijsmiddel op basis van een testresultaat. De testresultaten worden hierbij verstrekt door de uitvoerder van de test (de GGD of een privaat teststation).

Betrokkene installeert de CoronaCheck app op de smartphone[7] via de Apple App Store of de Google Play Store. Na installatie zoekt de CoronaCheck app contact met de configuratieserver van VWS, om daar de meest recente instellingen en actueel sleutelmateriaal op te halen.

Indien de test is afgenomen door een private testaanbieder ontvangt betrokkene, zodra de negatieve testuitslag beschikbaar is, een ophaalcode van de testaanbieder. Vervolgens vult

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

betrokkene in de CoronaCheck app deze ophaalcode in en ontvangt een verificatiecode om het ophalen van de testuitslag te bevestigen. Het genereren en verstrekken van de ophaalcode en de verificatiecode valt buiten de scope van deze DPIA. Het ophalen van de testuitslag valt wel binnen de scope van deze DPIA.

Indien de negatieve test is afgenomen door een GGD kan betrokkene zijn of haar testuitslag inzien en een testbewijs genereren door met DigiD in te loggen, via een link in de app. Dit vindt plaats via de TVS die door DICTU voor BZK wordt geëxploiteerd. Dit inlogproces vindt verder plaats buiten de CoronaCheck app en valt buiten de scope van deze DPIA. De techniek van de uitwisseling met een GGD wordt beschreven in paragraaf 8.3.

Het teststation of de GGD voorziet vervolgens in een door middel van een gekwalificeerde elektronische handtekening ondertekende uitslag. Deze ondertekening valt buiten de scope van deze DPIA. Via de CoronaCheck app haalt betrokkene deze ondertekende uitslag op. De signing servers controleren dan of de uitslag inderdaad afkomstig is van de testaanbieder. Dit laatste stukje valt wel binnen de scope van deze DPIA.

Vervolgens kan betrokkene ervoor kiezen een QR-code te genereren op basis van de opgehaalde testuitslag. De CoronaCheck app stuurt de uitslag dan naar de aan de app gekoppelde signing servers. De signing servers ondertekenen de uitslag namens de minister van VWS, maar alléén indien de opgehaalde informatie voldoet aan de vereisten die op Europees en nationaal niveau aan het EU DCC en Coronatoegangsbewijs worden gesteld. Vervolgens sturen de signing servers het testbewijs terug naar de CoronaCheck app, waar de gegevens worden opgeslagen. Indien de opgehaalde informatie niet voldoet aan de Europese en nationale vereisten, dan wordt geen testbewijs met een QR-code gegenereerd.

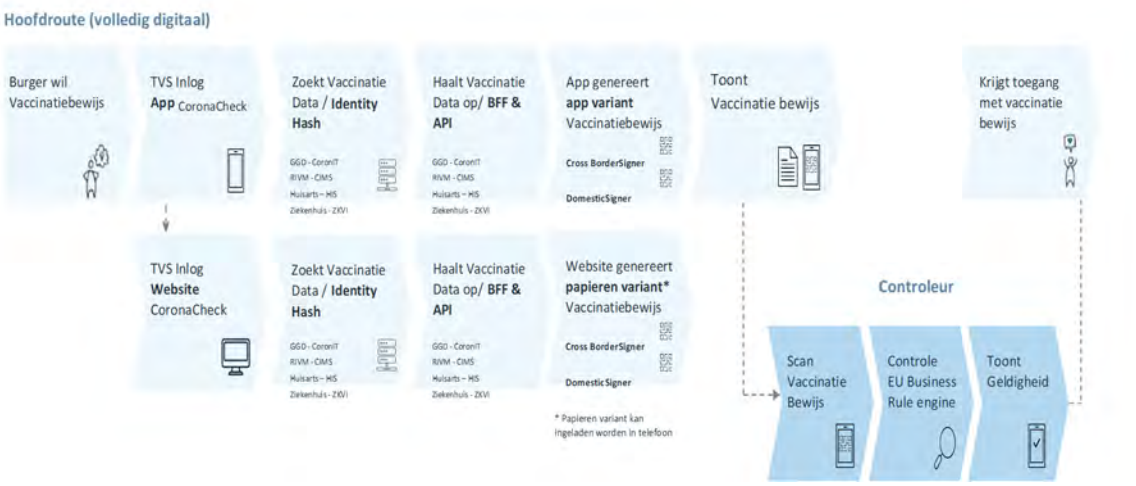
#### *Test – Digitale route fysiek Bewijsmiddel*

De stappen en bronsystemen voor deze route zijn hetzelfde als in de route voor een digitaal Bewijsmiddel in de CoronaCheck App, met het verschil dat de informatie uitwisseling niet plaatsvindt vanuit de CoronaCheck app, maar vanuit de Website (https://coronacheck.nl ). Ook wordt op de Website het Bewijsmiddel in de vorm van een QR-code gegenereerd, die door de persoon kan worden afgedrukt (in tegenstelling tot wanneer betrokkene gebruik maakt van de CoronaCheck app en enkel een digitaal Bewijsmiddel wordt gegenereerd). Hierdoor beschikt betrokkene over een papieren Bewijsmiddel. De vanuit de Website opgehaalde gegevens worden niet in de Website opgeslagen. Zodra betrokkene de browser sluit (al dan niet nadat een Bewijsmiddel is gegenereerd en geprint) zijn de gegevens niet meer beschikbaar. Indien de browser 24 uur open staat, dan krijgt betrokkene een melding dat zijn sessie is verlopen en dat de gegevens niet meer beschikbaar zijn.

### 3.3 Digitale route voor Bewijsmiddel op basis van vaccinatiebewijs

In onderstaande figuur is het proces opgenomen voor het genereren van een Bewijsmiddel op basis van een (voltooide) vaccinatie van betrokkene. Zowel voor de route via CoronaCheck (digitaal Bewijsmiddel) als via de Website (https://coronacheck.nl) (fysiek Bewijsmiddel). Voor de

overzichtelijkheid is de eerste stap uit de verwerking (het installeren van de CoronaCheck App) weggelaten.




*Figuur 2 Bewijsmiddel vaccinatie via CoronaCheck en coronacheck.nl*

### *Vaccinatie – Digitale route digitaal Bewijsmiddel via CoronaCheck app*

Deze paragraaf beschrijft het proces waarbij gebruik wordt gemaakt van de CoronaCheck app voor het genereren van een EU DCC of Corornatoegangsbewijs op basis van vaccinatie. De vaccinatiegegevens worden hierbij verstrekt door het RIVM (beschikt naar schatting over 82 % van de vaccinatiegegevens[8]) of de vaccineerder (zoals GGD, ziekenhuizen, huisartsen).

Na installatie van de CoronaCheck app zal betrokkene met zijn of haar DigiD moeten inloggen via de ToegangVerleningService (TVS) die door DICTU voor BZK wordt geëxploiteerd. Als dit succesvol verloopt zal de backend service van de CoronaCheck App van TVS een digitaal gewaarmerkt *token* ontvangen die het versleuteld burgerservicenummer (BSN) van de betrokkene bevat. Deze technische oplossing is gekozen omdat als het gaat om vaccinaties er sprake is van een groot aantal partijen en personen blijken niet altijd meer te weten bij welke partij men gevaccineerd is. Door middel van een technische oplossing (zie paragraaf 8.3) kan worden gezocht bij de verschillende vaccineerders. Met behulp van dit *token* worden in de gekoppelde vaccinatie-administraties de vaccinatiegegevens van betrokken opgevraagd.

Vervolgens kan betrokkene ervoor kiezen een QR-code te genereren op basis van de opgehaalde vaccinatiegegevens. De CoronaCheck app stuurt de uitslag dan naar de aan de app gekoppelde signing service. De signing service ondertekent de uitslag namens de minister van VWS, maar alléén indien de opgehaalde informatie voldoet aan de vereisten die op Europees en nationaal niveau aan een Bewijsmiddel worden gesteld. Vervolgens stuurt de signing service zowel de EU DCC als het

[8] Zoals bekend op moment van schrijven; 21-06-2021

Coronatoegangsbewijs terug naar de CoronaCheck app, waar de gegevens worden opgeslagen. Indien de opgehaalde informatie niet voldoet aan de Europese en nationale vereisten, dan worden geen Bewijsmiddelen verstrekt.

*Vaccinatie – Digitale route voor fysiek Bewijsmiddel*

In deze route is er geen sprake van de app, maar van een DigiD-inlog van betrokkene op een Website van VWS: https://coronacheck.nl. Ook dit resulteert in een digitaal gewaarmerkte *token* van TVS met behulp waarvan in de vaccinatie-administraties de relevante gegevens worden opgevraagd zoals in vorige paragraaf beschreven. Indien de gegevens voldoen aan de criteria van VWS voor de Bewijsmiddelen worden zowel het EU DCC als het Coronatoegangsbewijs in de vorm van een QR-code in een PDF-bestand aan de gebruiker ter beschikking gesteld. Deze kan er voor kiezen om deze af te drukken of elektronisch te bewaren. De via de Website opgehaalde gegevens worden niet in de Website opgeslagen. Zodra betrokkene de browser sluit (al dan niet nadat een Bewijsmiddel is gegenereerd en geprint) zijn de gegevens niet meer beschikbaar. Indien de browser 24 uur open staat, dan krijgt betrokkene een melding dat zijn sessie is verlopen en dat de gegevens niet meer beschikbaar zijn.

## 3.4 Digitale route Bewijsmiddel op basis van herstelverklaring

Voor een Bewijsmiddel op basis van een herstelverklaring geldt vooralsnog dat deze alleen worden uitgegeven op basis van een positief testresultaat. De benodigde positieve testresultaten worden door de GGD verstrekt voor zover een persoon door hen is getest.

Voor zowel het verkrijgen van een digitaal Bewijsmiddel via CoronaCheck App of een fysiek Bewijsmiddel via de Website (https://coronacheck.nl) op basis van een positief testresultaat, komt het proces nagenoeg overeen met de omschrijving zoals opgenomen voor negatieve testresultaten die worden verkregen van de GGD'en. Het verschil is dat de verwerking leidt tot het verstrekken van een herstelbewijs. Als het gaat om een herstelbewijs dan kan de QR-code al wel worden aangemaakt echter deze is pas na 11 dagen na datum van de positieve testuitslag geldig. Tot die tijd is het herstelbewijs grijs gemaakt zodat duidelijk is dat het nog niet geldig is.

## 3.5 Fysieke route voor fysiek Bewijsmiddel (HKVI)

Voor betrokkenen die een fysiek Bewijsmiddel wensen en geen gebruik kunnen maken van de printroute via de Website, is er een hulpleverlenersportaal ingericht (HKVI) waarmee hulpverleners een fysiek Bewijsmiddel kunnen verstrekken. De werking van het HKVI is in paragraaf 1.1 beschreven.

## 3.6 CoronaCheck Scanner applicatie

Zoals eerder beschreven kunnen controleurs in Nederland - naast nationale coronatoegangsbewijzen - ook EU DCC's uitlezen die door andere lidstaten zijn uitgegeven aan hun burgers om toegang te verlenen aan een evenement of locatie.
De CoronaCheck Scanner is zo gebouwd dat deze ook bij het uitlezen van de QR-code van een EU DCC, die meer gegevens bevat dan de QR-code voor nationaal gebruik, toch alleen de gegevens toont die te zien zijn bij het uitlezen van een nationaal coronatoegangsbewijs. De CoronaCheck Scanner toont "rood" of "groen" en de eerste letter voornaam en eerste letter achternaam,

geboortemaand en geboortedag van de gebruiker, zodat geverifieerd kan worden aan de hand van een fysiek identiteitsbewijs, dat de toonder van de EU DCC dezelfde persoon is als degene aan wie het uitgereikt is. Voor het beheer van CoronaCheck en CoronaCheck Scanner is een configuratieserver actief. Zo wordt bij het opstarten van de applicaties de configuratie opgehaald. Deze configuratie server bevat instellingen zoals de duur van de geldigheid van test-, vaccinatie- of herstelbewijzen en sleutels die gebruikt worden voor de beveiliging en het vaststellen van de betrouwbaarheid van het EU DCC. Ook bevat de configuratie server een mogelijkheid waarmee de service om voornoemde bewijzen te valideren tijdelijk of permanent beëindigd kan worden. Deze laatste mogelijkheid kan worden gebruikt als de inzet van de app definitief niet meer wenselijk wordt geacht.

De CoronaCheck Scanner kan – indien daartoe wordt besloten door de toezichthouder – tevens door de toezichthouder worden ingezet die deze kunnen gebruiken ter controle of de controleurs handelen volgens de geldende regels.

# 4. Verwerkingsdoeleinden

## 4.1 Verwerkingsdoeleinden EU DCC

De verordening treedt 1 juli 2021 in werking en verplicht de lidstaten tot de uitgifte van vaccinatie-, test- en herstelbewijzen. Door middel van een EU DCC kan het vrij verkeer van personen op een veilige wijze worden hersteld gedurende de pandemie en wordt voorkomen dat lidstaten een eigen oplossing kiezen die niet interoperabel is met die van andere lidstaten. Door middel van een trust framework kan de authenticiteit van een certificaat van een lidstaat in een andere lidstaat worden geverifieerd en kan fraude worden voorkomen. Het doel van de beoogde gegevensverwerking is daarmee om het vrij verkeer van personen tijdens de COVID-19-pandemie te faciliteren en te voorkomen dat mensen met een verhoogd besmettingsgevaar inreizen in de lidstaten. Dit gebeurt door de afgifte, verificatie en aanvaarding van interoperabele vaccinatie-, test- en herstelcertificaten teneinde het vrije verkeer tijdens de COVID-19-pandemie te vergemakkelijken.

## 4.2 Verwerkingsdoeleinden Coronatoegangsbewijs

Nederland heeft er belang bij dat niet-essentiële sectoren die tot nog toe aan de meeste COVID-19-pandemie gerelateerde restricties onderworpen zijn geweest (sport, cultuur, horeca) op gecontroleerde wijze weer, of meer, open kunnen.

# 5. Betrokken partijen

Er is een aantal partijen betrokken bij het genereren en gebruiken van een Bewijsmiddel. Onderstaande toelichting beschrijft welke partijen betrokken zijn en wat de rol van deze partijen is.

## 5.1 Gebruiker als betrokkene

De gebruiker als betrokkene is degene op wiens verzoek een Bewijsmiddel gegenereerd wordt. De daarvoor benodigde test-, vaccinatie en herstelgegevens worden alleen op diens verzoek door CoronaCheck of coronacheck.nl of via het hulpverlenersportaal opgevraagd bij de bronhouder en omgezet in een Bewijsmiddel (zowel EU DCC als een Coronatoegangsbewijs).

### 5.2 Hulpverlener als betrokkene (alleen bij HKVI)

De betrokkene is de vaccineerder of uitvoerder van de test die op verzoek van de gebruiker een Bewijsmiddel genereert door middel van HKVI. In beginsel zijn dit de artsen die verantwoordelijk zijn voor de vaccinaties of de tests, zij kunnen echter taken delegeren aan medewerkers (bijvoorbeeld doktersassistenten) die namens hen informatie in HKVI invoeren.

### 5.3 VWS en RIVM

CoronaCheck, de website coronacheck.nl, de CoronaCheck Scanner en het hulpverlenersportaal zijn ontwikkeld door VWS. De minister van VWS is de verwerkingsverantwoordelijke voor de verwerkingen van persoonsgegevens die bij het genereren van een Bewijsmiddel via CoronaCheck en coronacheck.nl en het hulpverlenersportaal worden verwerkt op grond van de verordening en op grond van nationale wetgeving inclusief de gerelateerde signing servers én de koppelvlakken met de overige verwerkingsverantwoordelijken zoals de bronsystemen die de gegevens aanleveren. VWS is daarmee ontvanger van de benodigde gegevens vanuit de bronsystemen van de vaccinatiezetters en uitvoerders van testen (zowel negatieve- als positieve testuitslagen). Ter verduidelijking: VWS heeft een dusdanig bepalende rol gespeeld in de totstandkoming van de specificaties en de aansluiteisen van de koppelvlakken met test-, vaccinatie- en hersteladministraties dat VWS als verwerkingsverantwoordelijke voor de opzet van deze koppelvlakken gezien moet worden. De bronhouders blijven zelfstandig verwerkingsverantwoordelijke voor de juistheid en kwaliteit van de door hen geleverde persoonsgegevens uit hun eigen administraties én de kwaliteit van de aanpassingen die zij in hun eigen systemen hebben aangebracht, met inbegrip van het voldoen aan de aansluiteisen om dit te faciliteren conform de specificaties van VWS.

RIVM (en daarmee de minister van VWS) is verwerkingsverantwoordelijke voor de vaccinatieadministratie die in CIMS wordt gevoerd. Als personen toestemming hebben gegeven aan de vaccinatiezetter voor de doorbreking van het beroepsgeheim dan worden de vaccinatiegegevens aan het RIVM doorgegeven en geregistreerd in CIMS. Dit dient als bronsysteem waar de gegevens voor een Bewijsmiddel op basis van een vaccinatie kunnen worden opgevraagd indien de persoon daarom verzoekt. Het RIVM is daarmee verstrekker van vaccinatiegegevens.

### 5.4 Uitvoerders testen: GGD’en, private testaanbieders

Uitvoerders van testen zijn zowel de GGD-en als private testaanbieders die testuitslagen aanleveren ten behoeve van het genereren van een Bewijsmiddel via CoronaCheck en coronacheck.nl of via het hulpverlenersportaal. Op verzoek van de persoon wordt bij de uitvoerders van de test de negatieve testuitslag opgehaald waarmee vervolgens een Bewijsmiddel kan worden gegenereerd. Testuitvoerders vervullen de rol van verwerkingsverantwoordelijke als het gaat om de eigen testadministraties. De testuitvoerders zijn daarmee verstrekkers van de gegevens zoals opgenomen in de negatieve testuitslag.

De herstelverklaringen worden momenteel alleen nog gebaseerd op positieve testuitslagen. Deze worden voorlopig alleen verstrekt door de GGD’en die de persoon hebben getest. Hiervoor geldt verder hetzelfde als bovenstaand is aangegeven. De GGD’en zijn de verwerkingsverantwoordelijken

voor die testadministraties en verstrekken de gegevens ten behoeve van het Bewijsmiddel gebaseerd op een positieve testuitslag (herstelbewijs).

Wanneer een testuitvoerder wil aansluiten op het in deze DPIA beschreven proces dient de testuitvoerder te voldoen aan de voorwaarden zoals gesteld door VWS in de aansluitvoorwaarden documentatie. Op deze manier worden testuitvoerders aangesloten die voldoen aan de privacy- en security eisen zoals gesteld door VWS. Op het stelsel worden vervolgens de nodige bewakingsslagen uitgevoerd (zoals toetsen beveiliging, bewaken op verandering en steekproeven)[9].

### 5.5 Uitvoerders van vaccinaties (GGD'en, ziekenhuizen, huisartsen, instellingsartsen)

Uitvoerders van vaccinaties zijn onder andere de GGD-en, de ziekenhuizen en de huisartsen die vaccinatiegegevens aanleveren ten behoeve van het genereren van een Bewijsmiddel via CoronaCheck en coronacheck.nl of zelf invoeren via het hulpverlenersportaal. Op verzoek van de persoon wordt bij de uitvoerder van de vaccinatie de vaccinatiegegevens opgehaald. Vaccinatiezetters vervullen de rol van verwerkingsverantwoordelijke als het gaat om de eigen vaccinatieadministraties en zijn daarmee verstrekkers van de gegevens zoals opgenomen in de vaccinatieadministratie.

Wanneer een vaccineerder of verklaarder van herstel wil aansluiten op het in deze DPIA beschreven proces dienen zij te voldoen aan de voorwaarden zoals gesteld door VWS zodat wordt voldaan aan de privacy- en security eisen zoals gesteld door VWS. De bijbehorende documentatie wordt momenteel opgesteld.

### 5.6 Ministerie van BZK

Het ministerie van BZK is verwerkingsverantwoordelijke voor een aantal bouwstenen die gebruikt worden binnen het beschreven proces. Het gaat daarbij om de TVS, een publieke routeringsvoorziening benodigd voor de DigiD-inlog en het gebruik van de Basisregistratie Personen (BRP) ten behoeve van het proces.

### 5.7 Verwerkers van VWS: Prolocation, Webhelp

- Prolocation beheert de configuratie server en back end systemen van VWS en tevens de signing servers (voor zowel Coronatoegangsbewijs als EU DCC) die door VWS worden ingezet. Prolocation is verwerker van VWS.
- Webhelp levert de benodigde helpdeskdiensten en is verwerker van VWS. De helpdesk fungeert als informatiepunt en ondersteunt burgers als ze vastlopen bij de werking van de app. Daarnaast zorgen ze voor uitleg en doorverwijzing als burgers er tegenaan lopen dat de data die wordt opgehaald niet volledig of juist is. Ze verwijzen dan bijvoorbeeld naar de testuitvoerders, GGD en RIVM en leggen uit wat de burger kan doen. Daarbij worden geen persoonsgegevens verwerkt. Als de helpdesk de vraag niet direct kan beantwoorden dan wordt de vraag uitgezet, daarvoor worden de naam en de contactgegevens van de burger verwerkt zodat opnieuw contact kan worden opgenomen zodra een antwoord beschikbaar is.

[9] https://www.rijksoverheid.nl/onderwerpen/coronavirus-covid-19/algemene-coronaregels/cijfers-en-onderzoeken-over-het-coronavirus/coronacheck-voor-aanbieders-testen

### 5.8 Controleurs

Controleurs scannen met CoronaCheck Scanner het Coronatoegangsbewijs of het EU DCC van een burger van een andere lidstaat voor toegang tot een activiteit of voorziening, waarvoor onder artikel 58ra, eerste lid, Wpg een toegangsbewijs mag worden gevraagd aan Nederlandse burgers. In CoronaCheck Scanner worden geen persoonsgegevens vastgelegd. De controleur krijgt bij het scannen van een EU DCC van een burger van een andere lidstaat te zien of de persoon beschikt over een geldig certificaat door middel van een groen of een rood scherm in CoronaCheck Scanner. Groen betekent dat de persoon beschikt over een geldig EU DCC. Rood betekent dat de persoon niet beschikt over een geldig EU DCC.
Een controleur controleert aan de hand van het identiteitsbewijs van de persoon of het EU DCC 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 worden getoond als het EU DCC wordt gescand. Deze set aan identificerende gegevens is beperkter dan de gegevens die de QR-code van de EU DCC moet laten zien in geval van controle bij reizen naar een andere lidstaat. Hier is bewust voor gekozen aangezien dit de mogelijkheid tot herleidbaarheid van de persoon vermindert en meer gegevens voor het verkrijgen van toegang tot bijvoorbeeld een evenement niet noodzakelijk zijn. Dit is anders bij controle als de persoon reist naar een andere lidstaat of bij een grenscontrole. Voor Nederlandse burgers geldt dat zij binnen Nederland enkel gebruik kunnen maken van het nationale coronatoegangsbewijs en geen gebruik kunnen maken van het EU DCC.

## 6. Belangen bij de gegevensverwerking

### 6.1 Belangen bij EU DCC

- De lidstaten en daarmee Nederland hebben een groot belang bij het verder kunnen verruimen van het vrije verkeer van personen op een veilige en zorgvuldige wijze. Het voorkomen dat er sprake is van inreizigers met een verhoogd besmettingsrisico is daarbij een belangrijk onderdeel. Het is daarvoor van belang dat het risico op besmetting met COVID-19 kan worden beheerst. Het Europees (technisch) kader voor de uitgifte van interoperabele certificaten inzake COVID-19-vaccinatie, -testen en –herstelbewijzen bevat daarom een infrastructuur waarmee de authenticiteit van een certificaat kan worden geverifieerd door de lidstaat. Tevens moeten de lidstaten voldoen aan de verplichtingen vanuit de verordening.
- De betrokkene zelf heeft er belang bij dat de bewegingsvrijheid binnen de EER wordt verruimd en reizen naar andere lidstaten mogelijk wordt zonder allerlei extra beperkende maatregelen zoals quarantaine. Het is ook in het belang van de persoon dat het risico op besmetting wordt verlaagd.
- De bronhouders hebben er belang bij dat ze op verzoek van de persoon die door hen is gevaccineerd of getest de gegevens kunnen leveren die noodzakelijk zijn voor het genereren van een EU DCC. Zij voldoen daarmee aan de verplichting vanuit de verordening. Daarnaast is het van groot belang voor de bronhouders dat ze op zorgvuldige wijze omgaan met het beroepsgeheim dat op hen rust.

### 6.2 Belangen bij Coronatoegangsbewijs

- Nederland heeft er belang bij dat niet-essentiële sectoren die tot nog toe aan de meeste COVID-19-pandemie gerelateerde restricties onderworpen zijn geweest (sport, cultuur, horeca) weer, of meer, open kunnen.
- De betrokkenen zelf heeft er belang bij dat hij weer van sportwedstrijden, culturele voorstellingen etc. kan genieten.
- De sport- en cultuurinstellingen en -bedrijven en horeca-ondernemers hebben er belang bij dat zij weer meer gelegenheid hebben om open te gaan en meer mensen te ontvangen.

## 7. Verwerkingslocaties

De verwerkingen vinden binnen de EER plaats, de middelen die nodig zijn als onderdeel van de volledige werking van het systeem om van een testuitslag of een vaccinatieattest een Coronatoegangsbewijs of een EU DCC te maken, dit zijn de configuratieserver (die op zichzelf geen persoonsgegevens verwerkt, maar daar wel van belang voor is) en de signing service, maar ook ondersteunende firewalls, logging servers en proxy servers staan in Nederland bij leverancier Prolocation.

De verwerkingen vinden zoals beschreven binnen de EER plaats, met dien verstande dat het kan voorkomen dat een gebruiker zijn of haar smartphone buiten de EER brengt en dat het deel van de verwerking die in de CoronaCheck App zelf plaatsvindt daardoor ook buiten de EER kan plaatsvinden. Dit valt echter buiten de invloedssfeer van VWS. Daarbij is het de vraag of er niet eerst sprake is van doorgifte in de zin van art. 44 AVG als de betrokkene een QR-code laat scannen buiten de EER. In de privacyverklaring zal een tekst worden opgenomen om de betrokkenen op dit punt te informeren.

Tenslotte voorziet de Verordening in de mogelijkheid om certificaten af te geven voor overzeese gebiedsdelen, waaronder die van Nederland (via een verwijzing naar art. 355 lid 2 Verdrag van de werking van de Europese Unie). Voor de afgifte van certificaten voor de overzeese gebiedsdelen zal een aparte DPIA worden opgesteld.

## 8. Techniek en methode van gegevensverwerking

Onderstaand wordt, voor zover nog niet uitgewerkt in voorgaande paragrafen, beschreven op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Tevens wordt benoemd of sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big-data verwerkingen.

Voor alle genoemde routes geldt dat het in de invloedssfeer van VWS ligt om deze geheel of gedeeltelijk af te schakelen, bijvoorbeeld door geen Bewijsmiddelen meer uit te geven en in het geval van de CoronaCheck app zelfs het kunnen tonen van bijvoorbeeld het Coronatoegangsbewijs uit te schakelen.

### 8.1 Route Digitaal Bewijsmiddel via CoronaCheck

- Mobiele telefoon (van betrokkene zelf);
- App Store (Apple of Google);
- Back-end systemen van VWS zoals configuratieserver en *signing servers*
- Koppelingen naar: GGD'en, RIVM, private testpartijen en zorg.
- Koppelingen naar: ToegangsVerleningService (TVS) en de BRP.

### 8.2 Route Fysiek Bewijsmiddel via coronacheck.nl

- Apparaat (computer, laptop, tablet) en *user agent* (browser) van betrokkene
- Website van VWS (coronacheck.nl)
- Back-end systemen van VWS zoals configuratieserver en signing service
- Koppelingen naar: GGD'en, RIVM, commerciële testpartijen en zorginstellingen.
- Koppelingen naar: ToegangsVerleningService (TVS) en de BRP.

Voor een aantal onderdelen die nog niet aan de orde zijn gekomen in voorgaande procesbeschrijving onderstaand een nadere uitwerking.

### 8.3 Ophalen brongegevens via gepseudonimiseerde bevraging

Met name voor de vaccinatiegegevens geldt dat de betrokkenen die de gegevens wil opvragen om een Bewijsmiddel aan te maken niet altijd weet in welke vaccinatieadministratie zijn of haar gegevens zijn opgenomen (omdat de eerste vaccinatie mogelijk in een andere administratie is opgenomen dan de tweede of omdat men niet goed weet onder wiens verantwoordelijkheid de vaccinatie is uitgevoerd). Om toch te kunnen zorgen dat de persoon kan beschikken over een EU DCC en Coronatoegangsbewijs is de volgende oplossing ontwikkeld. Na DigiD verificatie van de persoon wordt door middel van een gepseudonimiseerde bevraging van de relevante administraties, de vaccinatie-/test-/herstelgegevens van de gebruiker opgevraagd bij alle (potentieel) relevante partijen, met uitzondering van de private teststations (want daarvan zal de gebruiker altijd weten waar zijn testgegevens voorhanden zijn). Kort weergegeven is er sprake van de volgende stappen:

- De gebruiker logt door middel van DigiD in op CoronaCheck of coronacheck.nl
- Met behulp van de DigiD-identificatie én authenticatie worden – op basis van het BSN - in de BRP de volgende gegevens opgevraagd:
    - Voornaam
    - Geboortenaam
    - Geboortedatum

- Met het BSN en deze BRP-gegevens wordt een cryptografische hash-waarde berekend met behulp van het SHA-256 algoritme. Omdat genoemde invoerdata een zekere mate van voorspelbaarheid heeft, is de maximale entropie van dit deel van de hash-waarde niet de 256 bits die het SHA-256 algoritme potentieel biedt, maar is deze gereduceerd tot ongeveer 58 bits in de meest conservatieve schatting[10], maar effectief waarschijnlijk 70 bits (dit heeft te maken met de structuur van het BSN, hoe uniek achternamen zijn en dat de geboortedata in een maximaal interval van 1906 tot 2021 zullen liggen).
- Om deze nog relatief lage entropie te adresseren wordt bij de berekening van de hash-waarde een voor de zorgaanbieder unieke *salt* gebruikt (ook wel *shared secret* genoemd) die de entropie voor derden verhoogt evenredig aan de lengte van de *salt*. Vooralsnog wordt uitgegaan van een totale entropie (voor derden die niet bekend zijn met de *salt*) van 384 bits of meer. Dit vormt samen de “UNOMI-token”
- Uit oogpunt van proportionaliteit worden eerst de bronhouders waarvan de grootste kans is dat zij de benodigde gegevens hebben bevraagd met deze “UNOMI-token”. De volgorde van bevraging is RIVM en GGD’en tegelijk, daarna de overige bronsystemen zoals huisartsen en ziekenhuizen. Opgemerkt moet worden dat in de scenario’s waarbij de bronhouder wel bekend is bij de gebruiker, maar dit geen commercieel teststation is, deze “UNOMI-token” nog steeds wordt ingezet, maar dan als verificatiebevraging of de gegevens ook echt aanwezig zijn zonder ze werkelijk al gevraagd te hebben. Dit ter minimalisatie van de verwerkte persoonsgegevens.

**Hash-waarden zijn controlegetallen voor tekenreeksen. Zij hebben de eigenschap dat veranderingen in een tekenreeks veranderingen in het controlegetal opleveren. Een bijzondere variant hiervan zijn cryptografische hash-waarden. Deze hebben als eigenschap dat de kleinste wijziging in de tekenreeks de grootst mogelijke verandering in het controlegetal opleveren, waardoor de kans dat met een soortgelijke tekenreeks hetzelfde controlegetal berekend wordt geminimaliseerd wordt.**

[10] Deze inschatting is gebaseerd op de volgende elementen:

- Geboortejaar en BSN zijn gerelateerd (BSN wordt opvolgend uitgegeven, niet willekeurig);
- In Nederland zijn ongeveer 300 000 unieke achternamen;
- Ieder jaar zijn er ongeveer 300 voornamen echt populair, wel worden voornamen gecombineerd, in deze inschatting wordt met het laatste geen rekening gehouden, wat deze conservatief maakt;
- Van het BSN zijn zeven cijfers relevant (soms acht, ook hierom is de inschatting daarom conservatief);

Het totale aantal combinaties is $10^7 * 365 * 300\,000 * 300 = 2^{58}$.

- Omdat dezelfde invoerdata én de *salt* bekend zijn bij de bronhouder kan per aanwezig dossier dezelfde hash-waarde berekend worden;
- Als gevolg hiervan is het voor een partij die een vaccinatie-administratie voert mogelijk om op basis van een vanuit de app aan deze partij verzonden hash-waarde een positief of negatief antwoord te geven of deze hash-waarde correspondeert met een dossier in deze administratie. De hash-waarde fungeert dus als een zoeksleutel (ook wel de "UNOMI-token"). Dit is de eerste opvraging.
- Indien de aanvrager voorkomt in de administratie komt er een bericht terug dat de persoon bekend is. Vervolgens vindt er enkel bij die bronhouder een tweede opvraging plaats, waarbij de eerdere hash-waarde gepaard gaat met het BSN ter verificatie. De gevraagde gegevens worden, bij succes, via een versleuteld bericht ("JWT-token") geleverd aan de CoronaCheck App.
- De toegepaste versleuteling van zowel het BSN in de tweede opvraging als de levering van de gegevens is conform het X25519 algoritme. Dit is een algoritme dat een hogere bescherming biedt dan de BIO voorschrijft. De gegevens zijn voorzien van een gekwalificeerde elektronische handtekening van de aanbieder.
- Dit is een zogenaamd asymmetrisch algoritme, wat betekent dat de toegepaste technologie inpasbaar is in PKI-infrastructuren en ook ondersteund wordt door de Transport Layer Security (TLS) standaard versie 1.3 (en waar dit niet mogelijk is met versie 1.2).
- De geleverde gegevens worden bij levering ondertekend met behulp van het CMS (PKCS#7) algoritme, ook hiervoor geldt dat dit inpasbaar is in (bestaande) PKI-infrastructuren;

**Entropie is, voor deze context, een maatstaf voor de mate waarin een tekenreeks uniek is. Ook wel de mate waarin deze tekenreeks (bijvoorbeeld één die de basis is voor een hash-waarde) door blind uitproberen geraden kan worden. Deze wordt gemeten in bits. 384 bits entropie betekent dat er $2^{384}$ mogelijke combinaties ten grond kunnen liggen aan een bepaalde hash-waarde.**

Op basis van de geleverde gegevens kan vervolgens via het eerder beschreven proces een Bewijsmiddel gegenereerd worden op verzoek van de persoon.

### 8.4 Route fysiek bewijsmiddel via hulpverlenersportaal (HKVI)

Er is een separaat webportaal ingericht voor hulpverleners. Het belangrijkste technisch detail is dat de gebruikersauthenticatie via UZI-passen of twee-factor-authenticatie plaatsvindt. Er vindt geen uitwisseling met andere bronhouders van test-, vaccinatie- of herstelgegevens plaats.

### 8.5 Toelichting rol trust framework EU

Het trust framework betreft de uitwisseling van informatie over de PKI-certificaten die gebruikt worden voor de gekwalificeerde elektronische handtekeningen gezet door de lidstaten om de EU-DCC's te ondertekenen. Dit met inbegrip van ingetrokken gekwalificeerde elektronische handtekeningen. Dit betekent dat er informatie wordt uitgewisseld op PKI-certificaat-niveau, maar niet op individueel EU-DCC niveau. Omdat VWS er voor kiest om QR-codes met een maximale geldigheidsduur van 28 dagen (met uitzondering van fysieke Bewijsmiddelen) uit te geven (die vernieuwd moeten worden op basis van het door VWS uitgegeven Bewijsmiddel), kiest VWS er ook

voor om, achteraf bezien, onjuist uitgegeven DCC's niet in te trekken maar "uit te laten doven", dus de vernieuwing te blokkeren. Bij de uitwisseling van intrekkingen van EU DCC's van andere EER-lidstaten is er een theoretische mogelijkheid dat er persoonsgegevens worden verwerkt, ook door VWS, maar deze situatie kan zich alleen voordoen als een andere EER-lidstaat zich niet aan de verordening houdt.

Omgekeerd wordt het EU Trust Framework gebruikt om de CoronaCheck Scanner te voeden met geldige sleutels (en informatie over ingetrokken sleutels). Dit vindt niet realtime online plaats, maar periodiek, waarbij een volledige set geldige sleutels van andere EER-lidstaten wordt gepubliceerd en de set van ingetrokken sleutels die anders nog geldig zouden zijn. Hierdoor kan de CoronaCheck Scanner offline EU DCC's verifiëren.

## 8.6 Is sprake van (semi-)geautomatiseerde besluitvorming?

Er is geen sprake van profilering of big data-verwerkingen. In deze verwerking is wel sprake van geautomatiseerde besluitvorming met significant effect op de betrokkene in de zin van art. 22 lid 1 AVG. Of een EU DCC of een Coronatoegangsbewijs al dan wordt niet gegenereerd treft de betrokkene in aanmerkelijke mate, nu dit effect heeft op de bewegingsvrijheid van de betrokkene binnen de EU en met betrekking tot binnenlandse activiteiten en evenementen, en vindt via de applicatie CoronaCheck App en via de Website https://coronacheck.nl geheel geautomatiseerd plaats. Voor de juridische waardering hiervan verwijzen wij naar Deel B van deze DPIA (paragraaf 15.10). Voor nu moet opgemerkt worden dat er sprake is van een mogelijkheid van menselijke tussenkomst (**via de route van het hulpverlenersportaal HKVI**) waarbij de persoon contact kan opnemen met de vaccinatiezetter of uitvoerder van de test die vervolgens via een speciaal ingericht hulpverlenersportaal (HKVI) de gegevens invoert en een bewijsmiddel genereert dat door de persoon kan worden opgehaald of wordt verstuurd via de post. Tevens is voorzien in een helpdesk voor met name die personen die er niet in slagen een bewijsmiddel te genereren maar er wel recht op menen te hebben omdat ze zijn gevaccineerd of getest.

## 8.7 Beveiliging

In Deel C is een meer uitgebreide beschrijving opgenomen van de (voor)genomen maatregelen. In deze paragraaf de hoofdlijnen van de gebruikte technische en organisatorische maatregelen:

### *Technische maatregelen*

- Pseudonimisering: met name bij de bevraging van de bronhouders van de test-, vaccinatie- en herstelgegevens wordt gebruik gemaakt van een geavanceerde pseudonimisering die het mogelijk maakt om meerdere bronhouders te bevragen over betrokkene zonder dat de bronhouders kunnen reconstrueren welke betrokkene het betreft.
- Versleuteling: bij alle uitwisselingen extern wordt er gebruik gemaakt van geavanceerde versleuteling van de persoonsgegevens in transport. Dit is ook zoveel mogelijk doorgezet bij uitwisselingen tussen interne technische componenten van het systeem. Daarnaast zijn de persoonsgegevens in de App in rust versleuteld.
- Compartimentering: er zijn zoveel mogelijke technische afscheidingen gemaakt tussen de technische componenten die per (deel)stap betrokken zijn. Dit is te vergelijken met

waterdichte compartimenten in een schip. Tussen deze compartimenten onderling vindt de communicatie versleuteld plaats.

- Dataminimalisatie:
    - In het Coronatoegangsbewijs zit het absolute minimum wat nodig is om dit te kunnen laten werken. Daarnaast is het nagenoeg onmogelijk om de betrokkene op basis van QR-code scans te volgen nu deze elke negentig seconden wisselt.
    - De CoronaCheck Scan App zal niet meer informatie tonen op basis van een EU DCC dan het op basis van een Coronatoegangsbewijs zal tonen.
    - De levensduur van het door VWS uitgegeven digitale EU DCC is zo gekozen (28 dagen) dat het mogelijk is frauduleuze digitale EU DCC's te laten verlopen zonder intrekkingssleutels via het EU Trust Framework te hoeven verspreiden.

*Organisatorische maatregelen*

- Sleutelbeheer: het beheer van sleutels voor cryptografie is traditioneel een achilleshiel van iedere toepassing van versleutelingstechnieken. Het beheer van de sleutels is uitbesteed aan een partij die dit tot een kerncompetentie heeft verheven: JUSTID (onderdeel van het Ministerie van Justitie en Veiligheid).
- Actieve monitoring tegen phishing: om phishing tegen te gaan vindt er actieve monitoring plaats van diverse appstores en het zich voordoen van phishing sites.
- In zijn algemeenheid vindt er actieve monitoring op de verwerking plaats door middel van een Security Operations Centre (SOC).
- Toepassing beveiligingsstandaarden: er wordt gewerkt conform BIO en NEN 7510, respectievelijk met maatregelen die het niveau van de BIO en NEN 7510 overstijgen, dienstverleners dienen ISO 27001 gecertificeerd te zijn en ISO 27002 geïmplementeerd te hebben.

Het wisselende gebruik van BIO, NEN 7510 en ISO 27001/27002 verdient toelichting:

- ISO 27001 en ISO 27002 zijn internationale normen voor managementsystemen op het gebied van informatiebeveiliging. ISO 27001 beschrijft met name de organisatie van de informatiebeveiliging waarin de zogenaamde "Plan, Do, Act, Check" cyclus een centrale rol vervult. ISO 27002 is een bibliotheek van voorbeelden van beleidskeuzes op het gebied van beveiligingsmaatregelen. Beide normen zijn ook opgenomen in de Pas-Toe-Of-Leg-Uit-lijst van het Forum Standaardisatie en als zodanig leidend voor de Rijksoverheid.;
- Voor ICT-partijen die zelf geen onderdeel van een zorgaanbieder of van de overheid zijn is het nagenoeg onmogelijk om te certificeren conform NEN 7510 of de BIO. Deze partijen kunnen zich wel conform ISO 27001 certificeren;
- NEN 7510 is een Nederlandstalig, zorgspecifiek profiel op de ISO-normen 27001/27002, deze is op grond van het Besluit elektronische gegevensverwerking verplicht voor zorgaanbieders. NEN 7513 is een aanvullende norm op het gebied van logging, opnieuw specifiek voor de Nederlandse zorg;
- BIO is een Nederlandstalig, overheidsspecifiek profiel op de ISO-normen 27001/27002, deze is op grond van de Circulaire toepassen Baseline Informatiebeveiliging Overheid in het digitale verkeer met het Rijk verplicht voor VWS.

Voor het invulsysteem voor zorgverleners (HKVI) is gekozen om deze conform NEN 7510 te beveiligen en de logging conform NEN 7513 uit te voeren. Het gaat om zorggegevens die met hetzelfde niveau van zorg bejegend moeten worden als elders in de zorg het geval is. Voor de overige componenten die leiden tot een toekenning of afwijzing van een Bewijsmiddel is gekozen om deze conform de BIO te beveiligen, waarbij er op punten verdergaande methoden zijn gekozen dan de BIO voorschrijft. Voor door VWS ingezette dienstverleners geldt dat deze zich conform ISO 27001/27002 dienen te beveiligen.

## 9. Juridisch en beleidsmatig kader

Onderstaand wordt de wet- en regelgeving met mogelijke gevolgen voor de gegevensverwerkingen benoemd.

- de Verordening (EU) 2021/953 van het Europees Parlement en de Raad betreffende een kader voor de afgifte, verificatie en aanvaarding van interoperabele COVID-19-vaccinatie-, test- en herstelcertificaten (digitaal EU-COVID-certificaat) teneinde het vrije verkeer tijdens de COVID-19-pandemie te faciliteren.
- Wet publieke gezondheid (Wpg)
- Tijdelijke wet maatregelen Covid-19 (wijziging Wpg)
- Tijdelijke regeling maatregelen Covid-19
- Wijziging van de Wet publieke gezondheid in verband met het stellen van tijdelijke regels over de inzet van coronatoegangsbewijzen bij de bestrijding van het virus SARS-CoV-2 (Tijdelijke wet coronatoegangsbewijzen).
- Wetsvoorstel Wijziging van de Wet publieke gezondheid in verband met enkele verbeteringen en preciseringen van de tijdelijke regels over de inzet van coronatoegangsbewijzen bij de bestrijding van het virus SARS-CoV-2.
- Regeling van de Ministers van Volksgezondheid, Welzijn en Sport, van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties tot wijziging van de Tijdelijke regeling maatregelen covid-19 in verband met de inzet van coronatoegangsbewijzen op basis van een negatieve testuitslag.
- Regeling van de Ministers van Volksgezondheid, Welzijn en Sport, van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties tot wijziging van de Tijdelijke regeling maatregelen covid-19 in verband met de inzet van coronatoegangsbewijzen op basis van vaccinatie of herstel.
- Regeling van de Minister van Volksgezondheid, Welzijn en Sport houdende tijdelijke bepalingen ter uitvoering van de Europese verordening over certificaten met betrekking tot covid-19 (Tijdelijke spoedregeling DCC).
- Wet op de geneeskundige behandelingsovereenkomst (WGBO)

## 10. Bewaartermijnen

Het uitgangspunt is dat gegevens zo kort mogelijk worden bewaard. In de hiernavolgende paragrafen worden de specifieke bewaartermijnen beschreven.

### 10.1 Digitaal Bewijsmiddel via CoronaCheck app

- De benodigde gegevens voor het genereren van een Bewijsmiddel die worden verkregen van de bronhouders worden voor de duur van de geldigheid van het Bewijsmiddel bewaard om tussentijds nieuwe QR-codes te kunnen laten ondertekenen door de signing servers van VWS. Deze geldigheidstermijnen, en daarmee de bewaartermijnen van de benodigde gegevens, zijn, ten tijde van het opstellen van deze DPIA, geconfigureerd in de configuratieservers als:
    - 96 uur voor negatieve tests;
    - 365 dagen voor vaccinatiegegevens;
    - 180 dagen voor herstelgegevens.
- De daadwerkelijke bewaartermijn van een Bewijsmiddel is daarmee afhankelijk van enerzijds hoe lang de betrokkene het Bewijsmiddel bewaart en anderzijds van beleidskeuzes ten aanzien van de termijn waarop een Bewijsmiddel geldig is.
- De bewaartermijn van intrekkingen in het European Trust Framework is conform art. 10 lid 5 van de verordening maximaal tot einde toepassingsduur van de verordening (30 juni 2022).

### 10.2 Fysiek Bewijsmiddel via Website (coronacheck.nl)

- De benodigde gegevens voor het genereren van Bewijsmiddel die worden verkregen van de bronhouders worden niet langer dan enkele minuten bewaard op de Website van VWS.
- Vervolgens beschikt de betrokkene over een fysiek document, dit is daarmee dan buiten de reikwijdte van deze DPIA geraakt. De bewaartermijn van dit document staat los van de geldigheidsduur van het Bewijsmiddel of de gekwalificeerde elektronische handtekeningen waarmee het is ondertekend en is aan de betrokkene om te bepalen.

### 10.3 Fysiek Bewijsmiddel via hulpverlenersportaal (HKVI)

De gegevens in het HKVI-portaal worden na toekenning van de Bewijsmiddelen verwijderd. De Bewijsmiddelen worden op papier uitgereikt aan betrokkene en geraken daarmee opnieuw buiten de reikwijdte van deze DPIA. De bewaartermijn van dit document staat immers los van de geldigheidsduur van het Bewijsmiddel of de gekwalificeerde elektronische handtekeningen waarmee het is ondertekend en is aan de betrokkene om te bepalen.

### 10.4 CoronaCheck Scanner

In de CoronaCheck Scanner zoals uitgegeven door VWS worden geen persoonsgegevens opgeslagen. De verordening verbiedt in art. 10 lid 4 verwerking anders dan voor het doel van verificatie van het EU DCC. Opslag van gegevens in de CoronaCheck Scanner zou hiermee in strijd zijn.

### 10.5 Secundaire gegevensverwerking

De meer ondersteunende persoonsgegevens (logging van IP-adressen van gebruikers) worden maximaal zeven dagen bewaard.
Uitzondering hierop is de logging van IP-adressen en de logins (UZI of anderszins) in HKVI (het hulpverlenersportaal voor de uitzonderingsroute). Deze worden conform NEN 7513 minimaal twee jaar bewaard (het maximum is ook twee jaar).

# B. Beoordeling rechtmatigheid gegevensverwerkingen

## 11. Rechtsgrond

Het EU DCC en het coronatoegangsbewijs worden zoals eerder omschreven via dezelfde routes en technische oplossingen gegenereerd voor de persoon die hierom verzoekt. Als het gaat om de grondslagen voor deze verwerking van de benodigde persoonsgegevens dan geldt dat deze voor de EU DCC voortvloeien uit de verordening en voor het Coronatoegangsbewijs zijn geregeld in nationale wetgeving. De grondslag is daarmee wettelijke plicht zoals bedoeld in art. 6 lid sub c AVG. Onderstaand wordt dit nader uitgewerkt.

### 11.1Grondslagen EU DCC

*Uitgifte van de EU DCC door de minister van VWS*

De EU DCC wordt verstrekt op grond van de verordening (artikel 3 tweede lid van de verordening) en geeft als taak aan de minister van VWS (of de door hem aangewezen instanties) de uitgifte van het EU DCC in digitale vorm of op papier. Omdat de verordening rechtstreeks werkt en de noodzaak tot verwerking van gegevens in het kader van de opgelegde taak evident is, is het niet nodig om hiervoor een aparte verwerkingsgrondslag in de wet op te nemen. In artikel 10 zesde lid van de verordening wordt degene die verantwoordelijk is voor de uitgifte aangewezen als verwerkingsverantwoordelijke. De minister van VWS is daarmee verwerkingsverantwoordelijke voor de uitgifte van het EU DCC.

*RIVM: verstrekken vaccinatiegegevens*

In de Tijdelijke wet coronatoegangsbewijzen is in artikel 6ba een delegatiegrondslag opgenomen waarmee regels kunnen worden gesteld ter uitvoering van bindende onderdelen van EU-rechtshandelingen. Momenteel wordt een ministeriële regeling voorbereid op basis van deze delegatiegrondslag waarin de grondslag voor het RIVM voor het verstrekken van de vaccinatiegegevens vanuit het CIMS is opgenomen. De inwerkingtreding is voorzien vóór de ingangsdatum van de verordening.

*Verstrekken gegevens door vaccinatiezetters en uitvoerders van de test*

De vaccinatiezetters en uitvoerders van de test hebben op basis van de WGBO een dossierplicht. Voor het verstrekken van de benodigde gegevens voor het genereren van een EU DCC is de grondslag opgenomen in artikel 10, zevende lid, van de verordening waar de facto een wettelijke leveringsplicht is opgenomen voor degene die de vaccinatie heeft toegediend of de test heeft uitgevoerd. Dit biedt tevens de grondslag voor het doorbreken van het beroepsgeheim (op basis van een wettelijke plicht, artikel 7:457 lid 1 WGBO).

*Secundaire gegevensverwerking*

Voor de secundaire verwerking van persoonsgegevens (de verwerking van IP-nummers door de servers van VWS) geldt dat deze inherent zijn aan het gebruik van internet als medium én voortvloeien uit de verplichting van art. 32 AVG die op de verwerkingsverantwoordelijke rust om

passende technische en organisatorische maatregelen te treffen én uit overweging 15 van de Verordening die betrouwbaarheid van het Bewijsmiddel een sleutelbegrip in de Verordening maakt. In de Tijdelijke wet coronatoegangsbewijzen is in artikel 6ba een delegatiegrondslag opgenomen waarmee regels kunnen worden gesteld ter uitvoering van bindende onderdelen van EU-rechtshandelingen. Momenteel wordt een ministeriële regeling (Tijdelijke spoedregeling DCC) voorbereid op basis van deze delegatiegrondslag waarin de grondslag voor het verwerken van secundaire gegevens is opgenomen. De inwerkingtreding is voorzien vóór de ingangsdatum van de verordening.

## 11.2 Grondslagen nationaal Coronatoegangsbewijs

*Uitgifte van het coronatoegangsbewijs door de minister van VWS*

De Tijdelijke wet coronatoegangsbewijzen regelt de inzet van toegangsbewijzen met als doel het heropenen van de samenleving. In artikel 58re lid 4 staat dat de minister van VWS zorg draagt voor de inrichting en het beheer van de applicaties en waarborgen treft om ervoor te zorgen dat met de applicaties uitsluitend betrouwbare resultaten getoond worden. In art. 58re lid 5 is de minister van VWS aangewezen als verwerkingsverantwoordelijke. De grondslag voor het verwerken van de daarvoor benodigde gegevens is geregeld in het wetsvoorstel Wijziging van de Wet publieke gezondheid in verband met enkele verbeteringen en preciseringen van de tijdelijke regels over de inzet van coronatoegangsbewijzen bij de bestrijding van het virus SARS-CoV-2. In artikel 58re lid 6 is de grondslag voor de minister opgenomen om persoonsgegevens, waaronder persoonsgegevens over de gezondheid te verwerken. Dit wetsvoorstel is 15 juni 2021 aangenomen door de Tweede Kamer. In de ministeriële regeling tot wijziging van de Tijdelijke regeling maatregelen covid-19 in verband met de inzet van coronatoegangsbewijzen op basis van een negatieve testuitslag (artikel 6.31) en in de ministeriële regeling tot wijziging van de Tijdelijke regeling maatregelen covid-19 in verband met de inzet van coronatoegangsbewijzen op basis van vaccinatie of herstel (artikel 6.31a) wordt geregeld welke persoonsgegevens mogen worden verwerkt. De regeling met betrekking tot coronatoegangsbewijzen op basis van een negatieve testuitslag is 5 juni 2021 in werking getreden. Vooralsnog treedt de regeling met betrekking tot coronatoegangsbewijzen op basis van vaccinatie of herstel in werking zodra stap 4 van het openingsplan geldt. Deze stap is tijdens de persconferentie van 18 juni 2021 aangekondigd per 26 juni 2021.

*RIVM: verstrekken vaccinatiegegevens*

De grondslag voor het verstrekken van de vaccinatiegegevens door het RIVM ten behoeve van een nationaal coronatoegangsbewijs is geregeld in het wetsvoorstel Wijziging van de Wet publieke gezondheid in verband met enkele verbeteringen en preciseringen van de tijdelijke regels over de inzet van coronatoegangsbewijzen bij de bestrijding van het virus SARS-CoV-2. Dit wetsvoorstel is 4 juni 2021 ingediend bij de Tweede Kamer. In de ministeriële regeling tot wijziging van de Tijdelijke regeling maatregelen covid-19 in verband met de inzet van coronatoegangsbewijzen op basis van vaccinatie of herstel (artikel 6.31a) wordt geregeld welke persoonsgegevens door het RIVM mogen worden verwerkt. Vooralsnog treedt deze regeling in werking zodra stap 4 van het openingsplan geldt.

*Verstrekken gegevens door vaccinatiezetters en testers*
Voor het verstrekken van de benodigde gegevens voor het genereren van een coronatoegangsbewijs voor de uitvoerder van de test, de toediener van het vaccin en de verklaarder van het herstel is de grondslag voor het verstrekken van de gegevens opgenomen in artikel 58e lid 6 van de Tijdelijke wet coronatoegangsbewijzen. Dit biedt tevens de grondslag voor het doorbreken van het beroepsgeheim (op basis van een wettelijke plicht, artikel 7:457 lid 1 WGBO).

*Uitlezen door controleur*
Voor het lezen van het elektronische of schriftelijke coronatoegangsbewijs wordt een door de minister beschikbaar gestelde applicatie gebruikt: de CoronaCheck Scanner (art. 58re, lid 3 Tijdelijke wet coronatoegangsbewijzen). De controleur kan de benodigde gegevens verwerken om te zien of het elektronisch of schriftelijk coronatoegangsbewijs geldig is (artikel 58re lid 6 Tijdelijke wet Coronatoegangsbewijzen, ). Dit is uitgewerkt in de ministeriële regeling tot wijziging van de Tijdelijke regeling maatregelen covid-19 in verband met de inzet van coronatoegangsbewijzen op basis van een negatieve testuitslag (artikel 6.31 lid 4) en in de ministeriële regeling tot wijziging van de Tijdelijke regeling maatregelen covid-19 in verband met de inzet van coronatoegangsbewijzen op basis van vaccinatie of herstel (artikel 6.31a lid 6 en artikel 6.31b lid 4).

*Uitlezen door toezichthouder*
Voor het lezen van het elektronische of schriftelijke Coronatoegangsbewijs wordt een door de minister beschikbaar gestelde applicatie gebruikt: de CoronaCheck Scanner (art. 58re, lid 3 Tijdelijke wet coronatoegangsbewijzen). Artikel 58ra lid 1 Tijdelijke wet Coronatoegangsbewijzen regelt dat bij ministeriële regeling regels kunnen worden gesteld voor het beschikken over een bewijsmiddel voor toegang tot activiteiten of voorzieningen. Artikel 58rd, tweede lid, onder a van de Tijdelijke wet Coronatoegangsbewijzen regelt dat in diezelfde ministeriële regeling regels gesteld kunnen worden over een verplichting voor personen om het coronatoegangsbewijs en geldig identiteitsdocument te tonen aan een toezichthouder.
In artikel 6.30 lid 2 van de Tijdelijke regeling maatregelen is opgenomen dat de persoon die deelname of toegang wenst bij aanvang van de deelname of de toegang tevens zijn coronatoegangsbewijs en zijn identiteitsdocument aan een toezichthouder vertoont op diens verzoek. Dit is uitgewerkt in de ministeriële regeling tot wijziging van de Tijdelijke regeling maatregelen covid-19 in verband met de inzet van coronatoegangsbewijzen op basis van een negatieve testuitslag (artikel 6.31 lid 4) en in de ministeriële regeling tot wijziging van de Tijdelijke regeling maatregelen covid-19 in verband met de inzet van coronatoegangsbewijzen op basis van vaccinatie of herstel (artikel 6.31a lid 6 en artikel 6.31b lid 4). Deze artikelen regelen dat de toezichthouder de gegevens, bedoeld in artikel 6.28, onderdeel b, door middel van de applicatie, bedoeld in artikel 58re, derde lid, van de wet kan verwerken om te zien of het elektronisch of schriftelijk coronatoegangsbewijs geldig is en zo ja, wat de gegevens zijn, bedoeld in artikel 6.28, onderdeel b, onder 1o.

*Secundaire gegevensverwerking*
Voor de secundaire verwerking van persoonsgegevens (de verwerking van IP-nummers door de servers van VWS) geldt dat deze inherent zijn aan het gebruik van internet als medium. In de

ministeriële regeling tot wijziging van de Tijdelijke regeling maatregelen covid-19 in verband met de inzet van coronatoegangsbewijzen op basis van een negatieve testuitslag (artikel 6.31 lid 3) en in de ministeriële regeling tot wijziging van de Tijdelijke regeling maatregelen covid-19 in verband met de inzet van coronatoegangsbewijzen op basis van vaccinatie of herstel (artikel 6.31a lid 5) is de verwerking van het IP-adres geregeld.

## 12. Bijzondere persoonsgegevens

Onderstaand wordt beoordeeld of één van de wettelijke uitzonderingen op het verwerkingsverbod met betrekking tot bijzondere persoonsgegevens van toepassing is. Tevens wordt beoordeeld of de verwerking van het BSN (wettelijk identificatienummer) is toegestaan

### 12.1 Wettelijke uitzondering verwerkingsverbod bijzondere persoonsgegevens

De gegevens die worden verwerkt ten behoeve van het genereren van het EU DCC en het coronatoegangsbewijs en die door middel van een QR-code worden getoond, bevatten tevens bijzondere persoonsgegevens, als bedoeld in art. 4, onderdeel 15 resp. art. 9, eerste lid, AVG aangezien ze betrekking hebben op de gezondheid van de persoon. Voor het verwerken van bijzondere persoonsgegevens geldt een verwerkingsverbod tenzij aan een van de voorwaarden uit artikel 9, tweede lid AVG is voldaan.
Voor deze voorgenomen verwerking is sprake van een wettelijke uitzondering als bedoeld in art. 9 lid 2 sub g, er is namelijk sprake van een verplichting op grond van het Unierecht en het lidstatelijk recht.

### 12.2 Burgerservicenummer

Het BSN wordt verwerkt. Deze verwerking valt binnen de reikwijdte van art. 10-11 Wet algemene bepalingen burgerservicenummer.

## 13. Doelbinding

***Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld***

Er is geen sprake van verdere verwerking in de zin van art. 6 lid 4 AVG nu er voor het EU DCC en het Coronatoegangsbewijs sprake is van verwerking op grond van een Unierechtelijke verplichting en op grond van lidstatelijk recht.

## 14. Noodzaak en evenredigheid

Onderstaand wordt beoordeeld of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Hierbij wordt ingegaan op proportionaliteit en subsidiariteit.

### 14.1 Proportionaliteit

De vraag die moet worden beantwoord is of de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding staan tot de verwerkingsdoeleinden. Voor de beoordeling van de proportionaliteit van de voorgenomen verwerking zijn op basis van de jurisprudentie van het EHRM en de opinies van de WP29 (de voorganger van de EDPB) de belangrijkste criteria:

a) Niet in strijd met een wettelijke bepaling;
b) Een legitiem doel nastreven;
c) Noodzakelijk in een democratische samenleving.

**a. Niet in strijd met een wettelijke bepaling**

Wij hebben geen wettelijke bepalingen geconstateerd die in strijd is met de voorgenomen verwerking door middel van de inzet van de CoronaCheck app, coronacheck.nl of de route via het hulpverlenersportaal.

**b. Een legitiem doel nastreven**

Het doel wat nagestreefd wordt met het EU DCC is de bewegingsvrijheid van personen in de EER te verruimen nu deze zijn ingeperkt vanwege de COVID-19 pandemie. Het nagestreefde doel is dus het (gecontroleerd) bevorderen van het vrij verkeer van personen (artikel 21 VWEU). Als zodanig is evident dat de Verordening (EU 2021/0068) een legitiem doel nastreeft en in het verlengde daarvan de voorgenomen verwerking dit evenzeer doet.
Het doel dat nagestreefd wordt met de inzet van het Coronatoegangsbewijs voor nationaal gebruik is zorgen dat activiteiten en voorzieningen in tijden van COVID-19 sneller weer verantwoord plaats kunnen vinden. Met een Coronatoegangsbewijs kunnen personen toegang krijgen tot activiteiten en voorzieningen. De Tijdelijke wet coronatoegangsbewijzen bestaat uit een aantal artikelen die voor tijdelijke duur zijn toegevoegd aan de Wet publieke gezondheid. 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. Voor zowel de inzet van de EU DCC als het coronatoegangsbewijs geldt dat wordt nagestreefd de door de COVID-19 pandemie beperkte vrijheden te verruimen op een gecontroleerde wijze zodat wordt voorkomen dat het aantal besmettingen toeneemt door besmette inreizigers of deelnemers aan binnenlandse activiteiten op bovenstaande terreinen.

**c. Noodzakelijk in een democratische samenleving**

Dit criterium valt uiteen in drie subcriteria:

- Dringende maatschappelijke noodzaak:
  Er is sprake van dringende maatschappelijke noodzaak tot het kunnen opheffen van de inperkingen van de bewegingsvrijheid van ingezetenen in Nederland, zowel binnen Nederland, als ter zake van het meer vrij over de landsgrenzen binnen de EER kunnen reizen.
- Proportionaliteit van het middel voor het doel:
  Het doel is betrokkenen met een objectiveerbaar substantieel lagere kans op het zijn van een verspreider van SARS-CoV-2, de ziekteverwekker die de oorzaak is van de COVID-19

pandemie, een bewijsmiddel te verschaffen dat het mogelijk maakt activiteiten te verrichten die momenteel onder de werking van de in Nederland en andere EER-lidstaten geldende beperkingen om genoemde pandemie te bestrijden, vallen. Om dit doel te bereiken is informatie over de gezondheidstoestand van betrokkene (negatieve test), of diens immuniteit tegen SARS-CoV-2 (vaccinatie- of herstelbewijs) onontbeerlijk. Dit doel is helder en het middel is passend om dit doel te bereiken. Alternatieve maatregelen zijn in de huidige situatie vooralsnog niet mogelijk.

- Relevante en toereikende redenen:
  Hiermee wordt een aanpak op basis van empirisch bewijs voorgestaan. Omdat dit een nieuwe situatie betreft kan dit slechts bereikt worden met beleidsevaluatie ná deze verwerkingen.

### 14.2 Subsidiariteit

De belangrijkste subsidiariteitsvraag is of de verwerkingsdoelen bereikt kunnen worden met een minder vergaande verwerking van persoonsgegevens.

In het licht van de beslisregels zoals die vastgelegd zijn in de verordening is het voor het EU DCC niet mogelijk dezelfde doelen te bereiken zonder de persoonsgegevens zoals benoemd in paragraaf 2 te verwerken. Voor de persoonsgegevens die niet expliciet in de verordening benoemd zijn (zoals het BSN en de IP-adressen) geldt dat zonder het gebruik van het BSN de juistheid van de verwerkte persoonsgegevens zeer snel in het geding zou raken en dat zonder verwerking van de IP-adressen het online en geautomatiseerd verstrekken van het EU DCC eigenlijk niet mogelijk is. Bij het verwerken van het BSN is door het gebruik van de cryptografische hash-waarden (paragraaf 8) dit ook vergaand geminimaliseerd.
Bij het ontwerp van CoronaCheck en coronacheck.nl voor nationaal gebruik is het uitgangspunt geweest dat de verwerking 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.
Het gegevensgebruik is hiermee zo minimaal mogelijk en toegespitst op het doel van de verwerking.

## 15. Rechten van betrokkenen

Onderstaand wordt aangegeven op welke wijze invulling wordt gegeven aan de rechten van de betrokkenen.

### 15.1 Transparantie (art. 12, 13 AVG)

Voor de versie van de CoronaCheck en coronacheck.nl die momenteel al in gebruik zijn (nu nog alleen voor een nationaal coronatoegansgbewijs op basis van een testuitslag) worden de personen 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. Het privacy statement voor de versie van CoronaCheck en coronacheck.nl die tevens de in deze DPIA voorgenomen verwerkingen bevatten (EU DCC en coronatoegangsbewijzen voor zowel vaccinatie, test als herstel)

wordt momenteel opgesteld en zal op dezelfde wijze ter beschikking worden gesteld. De source code van CoronaCheck en CoronaCheck Scanner en alle technische informatie zijn bovendien openbaar beschikbaar via GitHub.

Voor de route via het hulpverlenersportaal (HKVI) geldt dat de betrokkenen zelf de betreffende zorgaanbieder verzoekt om de benodigde gegevens in te voeren in het portaal en vervolgens een Bewijsmiddel op papier ontvangt. Hierin staan de verwerkte persoonsgegevens vermeld.

### 15.2 Notificatieplicht (art. 14 AVG)

Indien de verwerkingsverantwoordelijke persoonsgegevens van een ander verkrijgt, moet de betrokkene hiervan uiterlijk binnen vier weken van op de hoogte worden gesteld. Hierin is voorzien in het ontwerp van CoronaCheck en via https://coronacheck.nl doordat de persoon bij het ophalen de gegevens getoond krijgt en daarbij wordt aangegeven uit welke bron deze afkomstig zijn (zoals RIVM, GGD, private teststations, huisarts).

Voor de route via het hulpverlenersportaal (HKVI) geldt dat de persoonsgegevens niet afkomstig zijn van een andere partij, artikel 14 AVG is daarmee niet van toepassing.

### 15.3 Recht op inzage (art. 15 AVG)

In het huidige ontwerp wordt voorzien in het actief tonen van de door CoronaCheck of Website (https://coronacheck.nl) zelf verwerkte persoonsgegevens (met uitzondering van het IP-adres). Voor de overige gegevens geldt dat er inzageprocessen belegd zijn binnen het ministerie van VWS en/of de betrokken verwerkers. Voor de route via het hulpverlenersportaal (HKVI) geldt dat de betrokkene via het papieren bewijs kan zien welke gegevens zijn verwerkt.

### 15.4 Recht op rectificatie (art. 16 AVG)

In het geval de betrokkene constateert dat onjuiste persoonsgegevens die hem of haar betreffen verwerkt worden, is voorzien in een helpdeskfunctie waarbij de persoon ondersteuning wordt geboden bij welke stappen gezet moeten worden om de gegevens te corrigeren. De persoon kan dit vervolgens bij de zorgaanbieder die verantwoordelijk is voor het bronsysteem of het RIVM laten aanpassen indien de gegevens niet correct zijn. Voor de route via het hulpverlenersportaal (HKVI) geldt dat de zorgaanbieder al bekend is en de betrokkenen kan de gegevens laten aanpassen.

### 15.5 Recht op verwijdering (art. 17 AVG)

Voor de primaire gegevensverwerking geldt dat de betrokkene de verwerkte persoonsgegevens zelf uit de CoronaCheck App kan verwijderen. Voor het genereren van een papieren bewijs via https://coronacheck.nl geldt deze op de website zelf binnen enkele minuten verdwijnt. Als de sessie met de website zijn geldigheid heeft verloren, wordt deze verwijderd uit de browser (tenzij de gebruiker deze op tijd downloadt). Het coronatoegangsbewijs kan ook eerder verdwijnen wanneer de persoon de browser waarin het bewijs wordt getoond sluit.

Voor de afgeleide verwerkingen geldt met name voor de IP-adressen dat de bewaartermijn dusdanig kort is (zeven dagen) dat een verwijderingsverzoek doorgaans later tot besluitvorming zal leiden dan dat het nog ingewilligd kan worden.

Voor de IP-adressen van zorgverleners (hulpverlenersportaal) geldt dat deze conform NEN-7513 gelogd worden (minimaal twee jaar) en gezien de verwerkingsgrondslag uit een wettelijke verplichting voortvloeit een verwijderingsverzoek niet snel gehonoreerd zal kunnen worden. Dit geldt ook voor de logging van de UZI-pas logins. Hier zijn de gangbare AVG-complianceprocessen van VWS van toepassing. Voor het hulpverlenersportaal (HKVI) geldt verder dat de gegevens na het aanmaken van het Bewijsmiddel automatisch worden verwijderd.

### 15.6 Recht op beperking (art. 18 AVG)

Nu het recht op verwijdering onverkort kan worden toegepast door betrokkene door de QR-codes te wissen, is dit recht niet aan de orde voor de primaire verwerking van persoonsgegevens, respectievelijk niet aan de orde door de korte bewaartermijnen.

Voor de afgeleide verwerkingen van persoonsgegevens is het antwoord naar analogie van het recht van verwijdering dat dit voor de IP-adressen van burgers/ingezetenen evenzeer niet aan de orde is door de korte bewaartermijnen.
Dit met uitzondering van het hulpverlenersportaal met betrekking tot de verwerking van gegevens van zorgverleners, hier is de uitleg van paragraaf 15.5 analoog van toepassing.

### 15.7 Kennisgevingsplicht derden (art. 19 AVG)

De kennisgevingsplicht is van toepassing op doorgiftes aan derden aan wie gerectificeerde, verwijderde of aan een beperking onderhevige persoonsgegevens zijn doorgegeven. Hier is in de context van de door deze DPIA bestreken verwerkingen geen sprake van.

### 15.8 Recht op overdraagbaarheid (art. 20 AVG)

Het recht op overdraagbaarheid is in casu niet van toepassing nu de verwerkingsgrondslag die van een wettelijke plicht zoals bedoeld in art. 6 lid sub c AVG is en niet de in art. 20 lid 1 sub a AVG genoemde verwerkingsgrondslagen (toestemming of uitvoering van overeenkomst).

### 15.9 Recht van bezwaar (art. 21 AVG)

Het recht van bezwaar is in casu niet van toepassing nu de verwerkingsgrondslag die van een wettelijke plicht is zoals bedoeld in art. 6 lid 1 sub c AVG is en niet de in art. 21 lid 1 genoemde verwerkingsgrondslagen (uitvoering van taak van algemeen, respectievelijk gerechtvaardigd belang).

### 15.10 Verbod van geautomatiseerde besluitvorming (art. 22 AVG)

Het verbod op geautomatiseerde besluitvorming van art. 22 lid 1 AVG is niet van toepassing. De uitzonderingssituatie van art 22 lid 2 sub b AVG is namelijk van toepassing nu wordt voldaan aan de aanvullende eis van art. 22 lid 4 AVG. Laatstgenoemde eis is aanvullend in het geval van verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in art. 9 lid 1 AVG, in dat geval moet de uitzondering van art. 9 lid 2 sub g AVG van toepassing zijn en aanvullende waarborgen getroffen worden. Dit is het geval.

Deze waarborgen zijn:

- De betrokkene wordt reeds voor het nemen van het besluit de gelegenheid gegeven zich te vergewissen van de persoonsgegevens op basis waarvan de besluitvorming plaatsvindt;

- De betrokkene is in staat om zich over de regels die worden toegepast in de besluitvorming te informeren. Dit wordt opgenomen in de privacyverklaring.
- De betrokkene kan zich door middel van de route via het hulpverlenersportaal tot diens vaccinatiezetter of uitvoerder van de test wenden en langs die weg alsnog een Bewijsmiddel verstrekt krijgen indien de betrokkene aan de criteria voldoet. Dit brengt een menselijke tussenkomst met zich mee en is effectief een mogelijkheid om het besluit aan te vechten.

Op grond van het voorgaande komen we niet toe aan toepassing van art. 40 UAVG.

# C. Beschrijving en beoordeling risico's voor de betrokkenen, maatregelen en restrisico's

## 16. Risico's

In dit onderdeel worden de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen die worden voorzien beschreven en beoordeeld. Hierbij wordt, conform de richtlijnen van WP29 voor gegevenseffectbeoordelingen[11], uitgegaan van een intrinsiek risicobegrip. Daarmee wordt bedoeld dat de kans en de impact van de negatieve gebeurtenis beoordeeld worden zonder dat eventuele reeds genomen maatregelen meegenomen worden in de beoordeling. De kans en de impact zijn daarbij kwalitatief ingeschat, met een schaal die van "laag", "middelhoog" naar "hoog" loopt. Daarbij is de schaal van het risico als functie van kans en impact er één die van "zeer laag", "laag", "middelhoog", "hoog" naar "zeer hoog" loopt.

Het betreft hier gebeurtenissen die kunnen leiden tot met name:

- Het niet vrij binnen de EER kunnen reizen (onterechte weigering van het verstrekken van het Bewijsmiddel), dit is een belangrijk recht en een belangrijke vrijheid van ingezetenen van de EER;
- Identiteitsdiefstal en fraude (door het lekken van het BSN);
- Het onjuist of onrechtmatig verwerken van gezondheidsgegevens, meer concreet heeft dit (potentiële) gevolgen in de vorm van discriminatie, stigmatisering en uitsluiting van de betrokkene indien onbevoegden zich toegang tot de gegevens verkrijgen;
- Het niet kunnen uitoefenen van rechten van betrokkenen, en daarmee aantasting van de informationele zelfbeschikking van de betrokkene.

Het onterecht niet verstrekken van een Bewijsmiddel heeft evenzeer potentiële uitsluitingsgevolgen voor de betrokkene, deze kan niet ten volle participeren in de samenleving.

Het geheel overziende zijn de risico's beheersbaar, mits de voorgenomen maatregelen ook daadwerkelijk worden uitgevoerd. Één risico blijft hoog, de betrouwbaarheid van de verificatie van de betrokkene door middel van DigiD-midden is niet zo hoog als wenselijk zou zijn. De beperking hier is echter dat middelen met een hoger betrouwbaarheidsniveau nog niet breed beschikbaar zijn.

[11] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Deze gevolgen zouden niet kunnen ontstaan zonder de verwerkingen die ten grondslag liggen aan het (al dan niet) verstrekken van een Bewijsmiddel.

| ernst schade (impact) | | | | |
|---|---|---|---|---|
| | ernstige schade | middelhoog risico | hoog risico | zeer hoog risico |
| | enige | laag risico | middelhoog risico | hoog risico |
| | minimaal | zeer laag risico | laag risico | middelhoog risico |
| | | onwaarschijnlijk | redelijke kans | eerder wel dan niet |
| | | waarschijnlijkheid van schade (kans) | | |

Vervolgens is aan de hand van de maatregelen (niet genomen, voorgenomen of genomen) beoordeeld wat het restrisico is wat overblijft.

Om de leesbaarheid te verhogen zijn de risico's ingedeeld in procesoverstijgende risico's en risico's die duidelijk te relateren zijn aan processtappen zoals in deel A beschreven. Daarbinnen zijn risico's opgedeeld in de volgende categorieëen:

- Apparatuur
- Programmatuur
- Gegevens
- Organisatie
- Omgeving
- Dienstverleners
- Ketenpartners

De gekozen systematiek is een afgeleide van de in de BIO gehanteerde MAPGOOD-methodiek (Mens, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving, Dienstverleners). Hiervan is afgeweken nu de factor Mens vooral de betrokkene zelf is en de meer menselijke fouten in de Organisatie liggen besloten. De Ketenpartners zijn opgenomen omdat er veel afhankelijkheden van ketenpartners zijn.

## 16.1 Procesoverstijgend

| *#1. Technisch falen door andere factoren* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Hier moet gedacht worden aan bijvoorbeeld onvermoede interacties tussen software-componenten onderling en/of systeemsoftware. Als dit zich in de CoronaCheck App voordoet kan dit leiden tot het niet toonbaar zijn van het Bewijsmiddel, met navenant hoge impact.** |
| **Maatregelen: Vier-ogen principe, testen etc., continuous testing, devops** |
| **De ontwikkelstraat van VWS werkt op basis van continuous integration en het vier-ogen-principe (toetsing door tweede persoon). Daarnaast vinden er geautomatiseerde kwaliteits- en beveiligingstests op de broncode plaats. De broncode wordt gepubliceerd onder een open source licentie en de relatie tussen de broncode en de gepubliceerde apps is verifieerbaar. Voorts zijn er mogelijkheden om publicatie van een foutieve versie van CoronaCheck App terug te draaien/te vervangen door een gecorrigeerde versie.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#2. Problemen in maatwerkcomponenten* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Fouten in de maatwerkprogrammatuur van zowel de App, webportaal als de back-end servers voor ophalen gegevens en/of de signing services kunnen leiden tot fouten in het bewijsmiddel, met grote impact op de betrokkene tot gevolg.** |
| **Maatregelen: Vier-ogen principe, testen etc., continuous testing, devops, defence in depth** |
| **De ontwikkelstraat van VWS werkt op basis van continuous integration en het vier-ogen-principe (toetsing door tweede persoon). Daarnaast vinden er geautomatiseerde kwaliteits- en beveiligingstests op de broncode plaats.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#3. Problemen in de gebruikte standaard componenten* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Fouten in de standaardcomponenten van zowel de App, webportaal als de back-end servers voor ophalen gegevens en/of de signing services kunnen leiden tot fouten in het bewijsmiddel, met grote impact op de betrokkene tot gevolg.** |
| **Maatregelen: Vier-ogen principe, testen etc., continuous testing, devops, defence in depth** |

| |
|---|
| **De ontwikkelstraat van VWS werkt op basis van continuous integration en het vier-ogen-principe (toetsing door tweede persoon). Daarnaast vinden er geautomatiseerde kwaliteits- en beveiligingstests op de broncode plaats.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#4. Uitval CoronaCheck App door programmeerfouten* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Het niet beschikbaar zijn van de App door een foute release kan het onmogelijk maken dat het bewijsmiddel getoond wordt, wat met name voor het EU DCC een grote impact voor de betrokkene met zich mee kan brengen. Het niet kunnen doen verifiëren van het Coronatoegangsbewijs kan eveneens een grote impact hebben op de betrokkene, ook omdat hiermee diens mogelijkheden tot sociale participatie worden ingeperkt.** |
| **Maatregelen: Vier-ogen principe, testen etc., continuous testing, devops, defence in depth** |
| **De ontwikkelstraat van VWS werkt op basis van continuous integration en het vier-ogen-principe (toetsing door tweede persoon). Daarnaast vinden er geautomatiseerde kwaliteits- en beveiligingstests op de broncode plaats.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#5. Uitval CoronaCheck Scanner door programmeerfouten* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Het niet kunnen verifiëren van het Bewijsmiddel kan een grote impact hebben op de betrokkene, ook omdat hiermee diens mogelijkheden tot sociale participatie worden ingeperkt.** |
| **Maatregelen: Vier-ogen principe, testen etc., continuous testing, devops, defence in depth** |
| **De ontwikkelstraat van VWS werkt op basis van continuous integration en het vier-ogen-principe (toetsing door tweede persoon). Daarnaast vinden er geautomatiseerde kwaliteits- en beveiligingstests op de broncode plaats.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#6. Ontbreken van inzageprocessen* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |

| |
|---|
| **Het recht op inzage (art. 15 AVG) is een cruciaal recht uit het gegevensbeschermingsrecht. Het ontbreken van een proces hiervoor, is behoudens andere maatregelen om dit recht op transparantie te kunnen effecturen, een ernstig risico voor de betrokkene.** |
| **Maatregelen: Er is geen inzageproces noodzakelijk nu gebruiker dit zelf kan.** |
| **De betrokken kan zijn gegevens inzien in de CoronaCheck App, hiermee is recht gedaan aan de autonomie van de betrokkene over diens gegevens.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#7. Ontbreken van versleuteling in rust* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Als het Bewijsmiddel niet versleuteld wordt opgeslagen in de App zou het denkbaar zijn dat andere applicaties op de mobiel (bijvoorbeeld malware) hier toch toegang toe zouden krijgen. Dit is geen incident op zichzelf, maar vooral een risicoverhogende factor.** |
| **Maatregelen: Versleuteling in de CoronaCheckApp** |
| **De gegevens worden versleuteld bewaard in de CoronaCheck App.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#8. Ontbreken van versleuteling in transport* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Geen incident op zichzelf, vooral een risicoverhogende factor, zeker nu de bevragingen van de bronhouders door de App over het "openbare" internet gaan.** |
| **Maatregelen: Versleuteling van het berichtenverkeer, server certificate pinning** |
| **De gegevens worden niet alleen tussen de CoronaCheck App, bronhouders en VWS servers versleuteld, maar ook binnen de VWS-servers onderling.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#9. Onnodig grote centrale databanken* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Het hebben van een grote centrale databank van vaccinatie- en testgegevens van Nederlandse ingezetenen is een risico op zichzelf. Een gevolg zou zijn dat VWS, als uitgever van het Bewijsmiddel én verstrekker van de controlemiddelen daarop (CoronaCheck Scanner App) in** |

| |
|---|
| **staat zou zijn grote delen van de bevolking te volgen bij het bezoeken van culturele evenementen en sportevenementen.** |
| **Maatregelen: Decentrale opzet** |
| **Door de CoronaCheck App zelf de gegevens op te laten halen en te laten ondertekenen én omdat de uitgelezen Bewijsmiddelen niet opgeslagen worden in de CoronaCheck Scanner App ontstaat er geen nieuwe centrale databank.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#10. Inbreuken via (data) ketenpartners* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Het incident zou hier zijn dat er sprake is van een inbreuk van buitenaf via systemen van ketenpartners. Dit is een specifieker risico dan "Inbreuken van buitenaf".** |
| **Maatregelen: Toetsen aansluitingen.** |
| **Er zijn uitgebreide aansluitvoorwaarden en er vindt toetsing conform een protocol plaats alvorens een ketenpartij wordt aangesloten.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#11. Ontbreken van rectificatieprocessen en doorzendingen* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Het recht op rectificatie (art. 16 AVG) is een cruciaal recht in het gegevensbeschermingsrecht en vloeit voort uit het juistheidsvereiste (art. 5 AVG). Bij rectificatie dient (conform art. 19 AVG) een doorzending van de rectificatie aan derden aan wie de onjuiste data eerder is verstrekt plaats te vinden. Het ontbreken van een proces hiervoor, is behoudens andere maatregelen om het recht op een juiste gegevensverwerking te kunnen effectueren, een ernstig risico voor de betrokkene.** |
| **Maatregelen: Er is een helpdesk.** |
| **Er komt een speciale helpdesk die betrokkenen helpen bij het verwerven van een juiste en verifieerbaar Bewijsmiddel als er problemen met de data bij BRP of bronhouders zijn.** |
| **Beperking/uitdaging: Dit is niet voor 23 juni.** |
| **Status maatregel: Voorgenomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#12. Ontbreken van verwijderingsprocessen en doorzendingen* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Het recht op verwijdering (art. 17 AVG) is een cruciaal recht in het gegevensbeschermingsrecht en vloeit voort uit de doelbindings- en proportionaliteitsvereisten (art. 5 AVG). Bij verwijdering dient (conform art. 19 AVG) een doorzending van het verzoek tot verwijdering aan derden aan wie de verwijderde data eerder is verstrekt plaats te vinden. Het ontbreken van een proces hiervoor, is behoudens andere maatregelen om het recht op een juiste gegevensverwerking te kunnen effectueren, een ernstig risico voor de betrokkene.** |
| **Maatregelen: De betrokkene kan de data verwijderen.** |
| **Bij verwijdering van de CoronaCheck App wordt ook de data verwijderd. Hiermee is recht gedaan aan de autonomie van de betrokkene over diens gegevens.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#13. Ontbreken van opschortingsprocessen en doorzendingen* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Het recht op opschorting (art. 18 AVG) is een cruciaal recht in het gegevensbeschermingsrecht en vloeit voort uit de doelbindings- en proportionaliteitsvereisten (art. 5 AVG). Bij opschorting dient (conform art. 19 AVG) een doorzending van het verzoek tot opschorting aan derden aan wie de opgeschorte data eerder is verstrekt plaats te vinden. Het ontbreken van een proces hiervoor, is behoudens andere maatregelen om het recht op een juiste gegevensverwerking te kunnen effectueren, een ernstig risico voor de betrokkene.** |
| **Maatregelen: De betrokkene kan de data verwijderen.** |
| **Bij verwijdering van de CoronaCheck App wordt ook de data verwijderd. Hiermee is recht gedaan aan de autonomie van de betrokken over diens gegevens.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#14. Afwezigheid van meldingsprocedure voor datalekken* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Het niet melden van een datalek betekent dat bij een datalek, zeker als het datalek voorzienbare schade voor de betrokkene kan opleveren, de betrokkene niet zelf mitigerende maatregelen kan treffen om de gevolgen van het datalek te trotseren.** |
| **Maatregelen: Er is een meldingsprocedure.** |

| |
|---|
| **Er zijn instructies voor de helpdesk over hoe te handelen bij het door een gebruiker gemeld worden van een datalek. Verder zijn de binnen de VWS gangbare instructies voor VWS-medewerkers hoe te handelen bij een (vermeend) datalek van toepassing.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#15. Doorgifte naar landen buiten de EER* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Doorgifte naar landen buiten de EER is in beginsel verboden (art. 74 AVG) omdat dit met een hoge mate van waarschijnlijkheid kan leiden tot een situatie waarin de betrokkenen hun rechten niet meer kunnen effectueren. Laatstgenoemde situatie wordt bij voorbaat als een ernstig risico gezien.** |
| **Maatregelen: Componenten anders dan de CoronaCheck App zelf uitsluitend in de EER laten werken.** |
| **Met uitzondering van de CoronaCheck App zelf kunnen alle componenten binnen de EER gehuisvest worden. De CoronaCheck App zal onvermijdelijk ook buiten de EER gebruikt worden. Aanvullende maatregel is hier de betrokkene over te informeren in de privacyverklaring.** |
| **Beperking/uitdaging: De CoronaCheck App zelf kan buiten de EER belanden, dit is onvermijdelijk voor o.a. Caribisch Nederland, maar ook voor reizigers die buiten de EER reizen.** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#16. Inbreuken van buitenaf* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Een inbreuk van buitenaf op bijvoorbeeld de signing servers zou tot een inbreuk op de persoonlijke levenssfeer van heel veel betrokkenen kunnen leiden, waarbij er gezondheidsgegevens in het geding zijn.** |
| **Maatregelen: Vier-ogen principe, testen etc., continuous testing, devops, defence in depth** |
| **De ontwikkelstraat van VWS werkt op basis van continuous integration en het vier-ogen-principe (toetsing door tweede persoon). Daarnaast vinden er geautomatiseerde kwaliteits en beveiligingstests op de broncode plaats.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#17. Gebruik van autorisaties van andere medewerkers* |
|---|
| **Impact: Laag** |

| |
|---|
| **Kans: Laag**<br>**Risico: Laag** |
| **Dit speelt met name rond HKVI, waar fouten bij autorisaties kunnen leiden tot het onterecht afgeven van Bewijsmiddelen. Omdat dit geen werkelijk negatief effect hoeft te hebben op betrokkenen is de impact hiervan laag.** |
| **Maatregelen: Integriteitstoetsing bij aanname, protocollen voor signaleren integriteitsproblemen, functiescheiding.** |
| **Er vindt een integriteitstoetsing van de personele bezetting binnen het programma plaats.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#18. Lekken van informatie* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Diefstal van gegevenssets is een groot probleem.** |
| **Maatregelen: Integriteitstoetsing bij aanname, protocollen voor signaleren integriteitsproblemen, functiescheiding.** |
| **Er vindt een integriteitstoetsing van de personele bezetting binnen het programma plaats. Daarnaast zijn er geen centrale databases.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#19. Onvoorzienbaar wegvallen personeel (ziekten, overlijden, ongeval, staking)* |
|---|
| **Impact: Middelhoog**<br>**Kans: Middelhoog**<br>**Risico: Laag** |
| **De beschikbaarheid van met name de CoronaCheck App zal niet snel in het geding komen, maar de uitgifte van nieuwe Bewijsmiddelen kan in het gedrang raken als er personele uitval in de beheerorganisatie van de betrokken VWS-systemen ontstaat. De kans hierop is laag ingeschat.** |
| **Maatregelen: voldoende redundantie in organisatie, deel van de redundantie is bereikt door specialistische uitbesteding.** |
| **De beheerorganisatie is deels al in staat om uitval van individuen op te vangen en is doende voldoende redundantie te organiseren om dit op termijn geheel te kunnen.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Voorgenomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#20. Diefstal (intern)* |
|---|
| **Impact: Hoog** |

| |
|---|
| **Kans: Hoog**<br>**Risico: Hoog** |
| **Diefstal van gegevenssets is een groot probleem.** |
| **Maatregelen: Integriteitstoetsing bij aanname, protocollen voor signaleren integriteitsproblemen, functiescheiding.** |
| **Er vindt een integriteitstoetsing van de personele bezetting binnen het programma plaats. Daarnaast zijn er geen centrale databases.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#21. Protocol niet gevolgd (opzettelijk)* |
|---|
| **Impact: Middelhoog**<br>**Kans: Middelhoog**<br>**Risico: Middelhoog** |
| **De factor mens blijft altijd een zwakke schakel. Denk aan het niet volgen van ontwikkel- en releaseprotocollen. Omdat dit over het algemeen ook achteraf te detecteren valt is hier een middelhoge impact ingeschat.** |
| **Maatregelen: Toetsen hanteren protocollen, vier-ogen principe.** |
| |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#22. Onzorgvuldige omgang met wachtwoorden* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Een onzorgvuldige omgang met wachtwoorden kan de integriteit en vertrouwelijkheid van het uitgifteproces van Bewijsmiddelen verstoren. Het kan ook leiden tot het aantasten van de integriteit van de CoronaCheck App en de CoronaCheck Scanner App.** |
| **Maatregelen: Twee-factor authenticatie, elimineren noodzaak van wachtwoorden, toetsen gebruik (logging).** |
| **Er wordt overal twee-factor authenticatie ingezet. Verder is er sprake van gebruik van wederkerige TLS-verbindingen waardoor wachtwoord gebruik geminimaliseerd wordt. Voor HKVI geldt dat er logging onform NEN 7513 is ingericht.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#23. Protocol niet gevolgd (onopzettelijk)* |
|---|
| **Impact: Middelhoog**<br>**Kans: Middelhoog** |

| |
|---|
| **Risico: Middelhoog** |
| **De factor mens blijft altijd een zwakke schakel. Denk aan het niet volgen van ontwikkel- en releaseprotocollen. Omdat dit over het algemeen ook achteraf te detecteren valt is hier een middelhoge impact ingeschat.** |
| **Maatregelen: Toetsen op consistente toepassing protocollen, vier-ogen principe.** |
| |
| **Beperking/uitdaging:** |
| **Status maatregel: Voorgenomen** |
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#24. Gebrekkig beheerbeleid* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Gebrekkig beheer van de betrokken Apps en/of de servers kan tot gebrekkige beschikbaarheid van nieuwe of vernieuwde Bewijsmiddelen leiden** |
| **Maatregelen: Hanteren best practices.** |
| **Het beheer is gemodelleerd naar ITIL v3 (o.a. incident management processen), daarnaast is de beheerorganisatie zo ingericht dat deze voldoet aan de eisen van NEN-7510, 7512 en 7513. Verder is er door de keuze van hostingpartners op technisch niveau hoogwaardig beheer ingericht. De beschikbaarheid van de VWS-servers wordt op een 4 000 parameters continu gemonitord.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#25. Onjuiste keuzes bij implementatie veiligheidsmanagementsystemen of ontbreken daarvan.* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Het toepassen van een veiligheidsmanagementsysteem sluit niet uit dat onjuiste keuzes gemaakt worden bij de toepassing daarvan, met gevolgen voor de beschikbaarheid, integriteit en de vertrouwelijkheid van de verwerking van persoonsgegevens.** |
| **Maatregelen: Motiveren van keuzes.** |
| **HKVI, configuratie- en signing servers zijn conform ISO 27001/27002 ingericht voor zover het om technische componenten van dienstverleners gaat. Daar waar door VWS zelf beheerd wordt gaat dit conform NEN 7510, 7512 en 7513.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#26. Slecht projectmanagement* |
|---|
| **Impact: Hoog** |

| |
|---|
| **Kans: Hoog**<br>**Risico: Hoog** |
| **Met name voor nieuwe releases geldt dat ontbrekend of slecht projectmanagement impact kan hebben op de kwalteit van de releases in termen van privacy en informatiebeveiliging.** |
| **Maatregelen: Hoogwaardig projectmanagement.** |
| **Er is een programma-organisatie, met per component een projectmanager. De componenten worden in lijn met "agile" methodieken ontwikkeld.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#27. Voorzienbaar wegvallen personeel (vakantie, ontslag)* |
|---|
| **Impact: Middelhoog**<br>**Kans: Middelhoog**<br>**Risico: Laag** |
| **De beschikbaarheid van met name de CoronaCheck App zal niet snel in het geding komen, maar de uitgifte van nieuwe Bewijsmiddelen kan in het gedrang raken als er personele uitval in de beheerorganisatie van de betrokken VWS-systemen ontstaat. De kans hierop is laag ingeschat.** |
| **Maatregelen: Goede vakantieplanning, voldoende redundantie in organisatie, deel van de redundantie is bereikt door specialistische uitbesteding.** |
| **De beheerorganisatie is deels al in staat om uitval van individuen op te vangen en is doende voldoende redundantie te organiseren om dit op termijn geheel te kunnen.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Voorgenomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#28. Fraude (intern)* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Diefstal van gegevenssets is een groot probleem.** |
| **Maatregelen: Integriteitstoetsing bij aanname, protocollen voor signaleren integriteitsproblemen, functiescheiding.** |
| **Er vindt een integriteitstoetsing van de personele bezetting binnen het programma plaats. Daarnaast zijn er geen centrale databases.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#29. Huisvesting* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog** |

| |
|---|
| **Risico: Hoog** |
| **Hier moet gedacht worden aan bijvoorbeeld een inbraak in het datacenter of het wegvallen van het datacenter.** |
| **Maatregelen: Fysieke beveiliging, uitwijk bij leveranciers.** |
| **Er zijn fysieke beveiligingsmaatregelen getroffen (eigen kooien, camerabewaking)** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#30. Nutsvoorzieningen* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Dit betreft uitval van elektriciteit, koelcapaciteit, connectiviteit.** |
| **Maatregelen: Noodstroomvoorzieningen, redundantie in connectiviteit.** |
| **Er is redundantie gecontracteerd.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#31. Externe calamiteiten* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Laag** |
| **Rampen als overstromingen en dergelijke.** |
| **Maatregelen: Uitwijkvoorzieningen, ook voor personeel** |
| **Er zijn drie uitwijklocaties, voor zowel servers als functionele uitwijk.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#32. Niet opleggen van beleid* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Het hebben van bevoegdheden uit hoofde van (verwerkers)overeenkomsten garandeert niet dat er daadwerkelijk gebruik wordt gemaakt van deze bevoegdheden.** |
| **Maatregelen: Operationaliseren van beleid** |
| **In tegenstelling tot een reguliere aanpak is hier sprake van directe operationele aansturing van de leveranciers vanuit het programma.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Hoog** |

| |
|---|
| **Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#33. Incidentele uitval dienstverleners* |
|---|
| **Impact: Middelhoog**<br>**Kans: Middelhoog**<br>**Risico: Middelhoog** |
| **Uitval van dienstverleners kan betekenen dat er geen nieuwe Bewijsmiddelen kunnen worden uitgegeven of Bewijsmiddelen niet kunnen worden vernieuwd. Als dit incidenteel is, zal de impact middelhoog zijn.** |
| **Maatregelen: Redundantie bij dienstverlener** |
| **De datacenters zijn driedubbel uitgevoerd.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#34. Niet passende (sub)verwerkersovereenkomsten* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Het niet hebben van passende (sub)verwerkersovereenkomsten kan er toe leiden dat persoonsgegevens verwerkt worden zonder de passende waarborgen van de AVG, in het bijzonder de passende technische en organisatorische maatregelen als bedoeld in art. 32 AVG.** |
| **Maatregelen: Passende verwerkersovereenkomst ( Prolocation, Webhelp)** |
| **De standaard-VWS verwerkersovereenkomsten worden ingezet.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#35. Structurele uitval dienstverleners* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Uitval van dienstverleners kan betekenen dat er geen nieuwe Bewijsmiddelen kunnen worden uitgegeven of Bewijsmiddelen niet kunnen worden vernieuwd. Als dit structureel is, zal de impact hoog zijn.** |
| **Maatregelen: Continuïteitsmanagement** |
| **Er is uitwijk, daarnaast zijn de datacenters driedubbel uitgevoerd.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#36. Niet nakomen contractuele afspraken* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Bij het niet nakomen van contractuele afspraken door dienstverleners ontstaat er de facto een situatie die gelijksoortig kan zijn aan het niet hebben van verwerkersovereenkomsten.** |
| **Maatregelen: Hoogwaardig contractmanagement** |
| **Dit is ingericht conform de staande contractmanagementprocessen van VWS** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

## 16.2 Installatie CoronaCheck App

| *#37. Onbeschikbaar zijn app in appstore* |
|---|
| **Impact: Laag**<br>**Kans: Laag**<br>**Risico: Laag** |
| **De impact voor de betrokkene bestaat hierin dat deze geen Bewijsmiddel kan genereren omdat de CoronaCheck App niet beschikbaar is. Over het algemeen zal de impact hievan laag zijn, tenzij de gebruiker dit op het laatste moment voor zijn of haar reis (bij EU DCC) of bezoek van een locatie (bij Coronatoegangsbewijs) pas het Bewijsmiddel wilde genereren. De kans schatten wij middelhoog.** |
| **Maatregelen: Terugvallen op Website (https://coronacheck.nl) en HKVI** |
| **Bij onbeschikbaarheid van de voor de betrokkene relevante appstore kan deze nog een fysiek Bewijsmiddel verkrijgen via de Website (https://coronacheck.nl) en/of het hulpverlenersportaal HKVI.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Middelhoog**<br>**Risico na maatregelen: Laag** |

| *#38. Valse app/phishing app* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **De impact voor de betrokken bestaat hierin dat deze vertrouwen schenkt aan apps van derden die gepresenteerd worden als de CoronaCheck App van VWS, deze zullen dat doorgaans met kwade bedoelingen (het verzamelen van persoonsgegevens voor phishing doeleinden, identiteitsdiefstal etc.) doen. De kans achten wij middelhoog omdat de ervaring met eerdere apps leert dat dit in de praktijk gebeurt.** |
| **Maatregelen: Communicatie/API keys voor back-end, client certificate pinning/korte communicatielijnen met Google/Apple/Detectie** |
| **De diverse ICT-componenten van de verwerking (zowel de CoronaCheck App als de configuratie- en de signing servers) hebben informatie over welke sleutelparen gebruikt** |

| |
|---|
| **kunnen worden voor de versleuteling van de onderlinge communicatie. Hierdoor wordt het wijzigen van componenten zonder dat dit opgemerkt wordt ernstig bemoeilijkt. Dit is een onderdeel van het "defence-in-depth" principe wat is toegepast.** |
| **Beperking/uitdaging: Uiteindelijk zal dit vooral reactief zijn. Ook certificate pinning is uiteindelijk niet onfeilbaar.** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

## 16.3 Verificatie identiteit gebruiker

| *#39. Authenticatiemethode gebruikers onvoldoende betrouwbaar* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Als men zich kan voordoen als een ander is het denkbaar dat gezondheidsgegevens van een ander persoon met de werkelijke gebruiker gedeeld worden en/of dat het Bewijsmiddel onbetrouwbaar wordt.** |
| **Maatregelen: eIDAS-hoog-conforme authenticatie kiezen.** |
| |
| **Beperking/uitdaging: Op korte termijn is er voor Nederlandse burgers geen online authenticatie-infrastructuur die e-IDAS-conform is beschikbaar.** |
| **Status maatregel: Niet genomen** |
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Middelhoog**<br>**Risico na maatregelen: Hoog** |

| *#40. TVS niet beschikbaar* |
|---|
| **Impact: Middelhoog**<br>**Kans: Middelhoog**<br>**Risico: Middelhoog** |
| **Een gevolg van een onbeschikbaar TVS is dat de Bewijsmiddelen die afhankelijk zijn van TVS (met name vaccinatie- en herstelbewijzen) niet afgegeven kunnen worden. Middelhoge impact omdat samenstellen gegevensset zelden tijdkritisch is, middelhoge kans (verstekwaarde).** |
| **Maatregelen: Afspraken beschikbaarheid TVS/DDoS-mitigatie** |
| **VWS is nog in gesprek met DICTU om dit te waarborgen. Daarnaast zijn er maatregelen getroffen om overvraging van TVS te voorkomen.** |
| **Beperking/uitdaging: Hier is een afhankelijkheid van DICTU (BZK)** |
| **Status maatregel: Voorgenomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

## 16.4 Opvragen brongegevens

| *#41. Bronhouders leveren onjuiste dossiergegevens* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Onjuiste gegevens in de test-, vaccinatie- en hersteladministraties zijn een risico. Het is bijvoorbeeld voorgekomen dat de geboortedatum als vaccinatiedatum is geregistreerd. Een dergelijke onjuistheid levert verderop in het proces een mogelijke weigering van het Bewijsmiddel op.** |
| **Maatregelen: Afspraken integriteit BRP, goede escalatieprocedure inregelen** |
| **Voor dit soort problemen wordt een helpdesk ingericht die burgers gaat helpen door middel van de uitzonderingsroutes toch een geldig en verifieerbaar Bewijsmiddel te krijgen.** |
| **Beperking/uitdaging: Dit is niet voor 23 juni gerealiseerd.** |
| **Status maatregel: Voorgenomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Middelhoog**<br>**Risico na maatregelen: Middelhoog** |

| *#42. Uitvragen gegevens over betrokkene bij bronhouders leidt tot (onrechtmatige) verstrekking aan bronhouders* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Dit risico bestaat eigenlijk vooral bij een Bewijsmiddel wat gebaseerd is op vaccinatiegegevens, omdat de betrokkene niet altijd zal weten in welke administratie hij of zij bekend is worden er meerdere bevraagd. Zonder maatregelen betekent dit dat de bronhouders van de bevraagde administraties automatisch zouden kunnen weten dat betrokkene bezig is zich een Bewijsmiddel te verschaffen.** |
| **Maatregelen: Ontwerp voorziet in stalted hash met entropie van 384 bits.** |
| **Zie paragraaf 8 voor een uitgebreide beschrijving van de salted hash die toegepast is bij het verzenden van de "UNOMI-token"** |
| **Beperking/uitdaging: Entropie voor bronhouders die wel bekend zijn met betrokkene, maar niet de gevraagde gegevens heeft is lager, maar nog steeds hoog genoeg om dit lage restrisico te rechtvaardigen.** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#43. Geen notificatie van betrokkene van verwerving gegevens van derdene (verplicht ex art. 14 AVG)* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Één van de rechten van betrokkenen van de AVG is het recht om verwittigd te worden van de verwerking van persoonsgegevens die door derden verstrekt zijn, met inbegrip van de oorsprong van deze gegevens (art. 14). Het hier niet aan voldoen is een inperking van de** |

| |
|---|
| **rechten van betrokkenen en als zodanig, op grond van overweging 75 AVG, al een risico voor de betrokkene.** |
| **Maatregelen: Bij ophalen gegevens laten zien bij welke bronhouders er gegevens worden gevraagd, ook hier helpdesk** |
| **In de CoronaCheck App wordt nadat de gegevens zijn opgehaald getoond welke gegevens bij welke bronhouder afkomstig zijn.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#44. BRP niet beschikbaar* |
|---|
| **Impact: Middelhoog**<br>**Kans: Middelhoog**<br>**Risico: Middelhoog** |
| **Het niet beschikbaar zijn van de BasisRegistratie Personen (BRP) is vervelend, maar niet onoverkomelijk bij kortdurende verstoringen.** |
| **Maatregelen: VWS-kopie van BRP om een DDoS-aanval het hoofd te kunnen bieden.** |
| **Met RvIG is overeengekomen dat er een noodscenario wordt gerealiseerd om een eventuele overbelasting van de BRP het hoofd te kunnen bieden. Dit noodscenario bestaat uit een beperkte schaduwkopie van de BRP. De beperking bestaat er in dat alleen gegevenselementen die van belang zijn voor het verstrekken van een Bewijsmiddel (voornamen, achternamen, geboortedatum) in deze schaduwkopie is opgenomen. Deze zal alleen ingezet worden bij piekbelastingen waarbij de BRP overvraagd dreigt te worden door bevragingen geïnitieerd door de CoronaCheck App.** |
| **Beperking/uitdaging: Zal een korte verstoring met zich meebrengen bij inzet.** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Laag**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Zeer laag** |

| *#45. TVS levert onjuist BSN in token* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **TVS is de DigiD-inlogvoorziening waarmee de identiteit van de betrokkene wordt geverifieerd (in de meeste gevallen). Tegelijkertijd levert deze het BSN van de betrokkene in de vorm van een fiche (“token”) aan de CoronaCheck App. Als hier een onjuist BSN wordt geleverd zal er een de facto persoonsverwisseling plaats kunnen vinden, respectievelijk (minder kwalijk) zal iedere verdere bevraging van bronhouders mislukken omdat er een BSN van een niet bestaande persoon als sleutel wordt gehanteerd. De oorzaak van onjuiste gegevens ligt dan weliswaar buiten de invloedssfeer van VWS, een verwerking van VWS wordt hier wel onjuist door.** |
| **Maatregelen: Afspraken integriteit TVS, goede escalatieprocedures inregelen** |
| **VWS is nog in gesprek met DICTU om dit te waarborgen.** |
| **Beperking/uitdaging: Hier is een afhankelijkheid van DICTU (BZK)** |
| **Status maatregel: Voorgenomen** |
| **Impact na maatregelen: Middelhoog** |

| |
|---|
| **Kans na maatregelen: Middelhoog**<br>**Risico na maatregelen: Middelhoog** |

| *#46. BRP levert verkeerde gegevens* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Een onjuiste gegevensverstrekking uit de BRP, bijvoorbeeld door verstrekking van een andere naam of een andere geboortedatum dan op het identiteitsbewijs van de betrokkene staat levert uiteindelijk een onbruikbaar Bewijsmiddel voor betrokkene op. Onvolkomenheden komen voor in de BRP, daarom is de kans middelhoog ingeschat.** |
| **Maatregelen: Afspraken integriteit BRP, goede escalatieprocedure inregelen** |
| **Voor dit soort problemen wordt een helpdesk ingericht die burgers gaat helpen door middel van de uitzonderingsroutes toch een geldig en verifieerbaar Bewijsmiddel te krijgen.** |
| **Beperking/uitdaging: Dit is niet voor 23 juni gerealiseerd.** |
| **Status maatregel: Voorgenomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Middelhoog**<br>**Risico na maatregelen: Middelhoog** |

## 16.5 Beoordelen brongegevens

| *#47. Problemen bij de business rules software/parametrisatie zelf* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Onjuiste business rules kunnen tot fout-negatieven leiden. Het niet kunnen krijgen van een Bewijsmiddel heeft grote impact op de betrokkene.** |
| **Maatregelen: Verificatie kwaliteit van inrichting, continu testen** |
| **Het programma is doende het pentesten geautomatiseerd in te regelen via een zogenaamde Kwetsbaarheden Automatiserings Tool (KAT), de uitkomsten waarvan geverifieerd zullen worden door menselijke tussenkomst.** |
| **Beperking/uitdaging: Zogenaamde "nuldaagse kwetsbaarheden/zero days". Kan ook geen broncode-onderzoek vervangen.** |
| **Status maatregel: Voorgenomen** |
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

## 16.6 Uitgifte Bewijsmiddel

| *#48. Onjuiste sleutels* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **De impact is hier hoog omdat het Bewijsmiddel niet als zodanig kan fungeren, wat een inperking van de reismogelijkheden van betrokkene leidt (in het geval van het EU DCC)** |

| |
|---|
| **respectievelijk het niet hebben van een bruikbaar Coronatoegangsbewijs en de daardoor verminderde sociale participatiemogelijkheden.** |
| **Maatregelen: Best practices voor sleutelbeheer toepassen (JUSTID)** |
| **Het sleutelbeheer is zijn geheel neergelegd bij een partij binnen de overheid die hier de meeste ervaring mee heeft. Dit is JUSTID die op basis van "best practices" dit uitvoert. De scheiding tussen JUSTID en de rest van de beheerorganisatie heeft hierbij een meerwaarde in termen van compartimentalisatie (opnieuw "defence-in-depth")** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#49. Specifieke sleutel voor bijzondere gevallen om een ping-back* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Hoog** |
| **Het European Trust Framework sluit niet uit dat door gebruik van bijzondre sleutelparen bij het zetten van de gekwalificeerde elektronische handtekening in het Bewijsmiddel het Bewijsmiddel toch volgbaar wordt bij raadplegingen. Dit is niet eenvoudig te realiseren en vergt opzet, maar is desalniettemin geen bij voorbaat te verwaarlozen kans. Een dergelijke surveillance kan gerekend worden tot een gebeurtenis met een hoge impact op de betrokkene.** |
| **Maatregelen: Gebruik OCSP verboden, op controleren (door volledige transparantie van EU gateway)** |
| **Er vindt monitoring plaats op het intrekken van gekwalificeerde elektronische handtekeningen. Voor Nederlandse Bewijsmiddelen is dit afgedekt, ook door inzet van JUSTID.** |
| **Beperking/uitdaging:** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

## 16.7 Uitlezen Bewijsmiddel

| *#50. Niet door gebruiker geautoriseerde uitlezing* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Leidt tot onrechtmatige inzage in gezondheidsgegevens van gebruiker.** |
| **Maatregelen: Meeste gebruikers hebben hun smartphone beveiligd met een pincode en/of biometrische toegang.** |
| **Communicatie naar gebruikers toe dat ze de beveiligingsmiddelen van hun smartphone ook echt moeten gebruiken.** |
| **Beperking/uitdaging: Is in huidige situatie lastig te beheersen voor VWS. Een aanvullende DigiD-login zou a) afdoen aan gebruiksvriendelijkheid en b) niet stroken met overweging 22 van de Verordening (geen ping-back).** |
| **Status maatregel: Voorgenomen** |

| |
|---|
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |

| *#51. Alternatieve uitleesapplicaties die opslaan* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Leidt tot onrechtmatige inzage in gezondheidsgegevens van gebruiker en daarmee een onrechtmatige verwerking van persoonsgegevens. Dit heeft een hoge impact op de betrokkene en de kans dat dit gebeurt is reëel.** |
| **Maatregelen: Communicatie, ook naar gebruikers/potentiële gebruikers (controleurs) toe. Verordening verbiedt dit ook duidelijk.** |
| **Er vindt bewaking op de app stores plaats in de zin dat er monitoring plaatsvindt of er geen alternatieve scan apps opduiken. Dit wordt in samenwerking met Logius gedaan.** |
| **Beperking/uitdaging: Dit valt niet helemaal te voorkomen.** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Middelhoog**<br>**Kans na maatregelen: Middelhoog**<br>**Risico na maatregelen: Middelhoog** |

| *#52. Misbruik van uitgelezen Bewijsmiddelen* |
|---|
| **Impact: Hoog**<br>**Kans: Hoog**<br>**Risico: Zeer hoog** |
| **Bij controles van de Bewijsmiddelen kunnen potentieel grote aantallen QR-codes uitgelezen worden, zonder maatregelen zou dit tot een onrechtmatige dataverzameling kunnen leiden.** |
| **Maatregelen: Dataminimalisatie in CoronaScanner App** |
| **In het ontwerp van de CoronaScanner App is er voor gekozen een minimale gegevensset in beeld te brengen.** |
| **Beperking/uitdaging: Dit is minder goed te voorkomen bij inzet alternatieve scanner applicaties.** |
| **Status maatregel: Genomen** |
| **Impact na maatregelen: Hoog**<br>**Kans na maatregelen: Laag**<br>**Risico na maatregelen: Laag** |