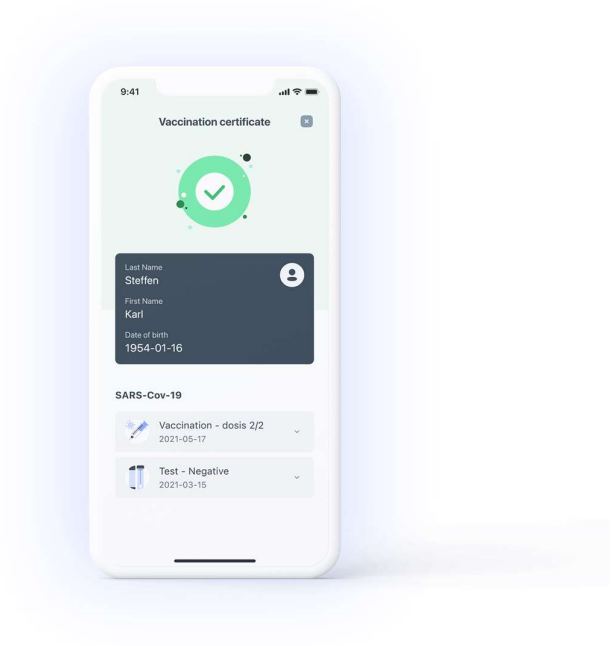
CovidScan applicatie België

Gegevensbeschermingseffectbeoordeling



Inhoud

Begrippen

Anonimiseren van gegevens	Het verwerken van persoonsgegevens op zodanige wijze dat de gegevens niet meer tot een specifieke betrokkene kunnen worden herleid en dus geen persoonsgegevens meer zijn.
AVG	De Algemene verordening gegevensbescherming (AVG) (Engels: General Data Protection Regulation (GDPR); de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende

	het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG) is een Europese verordening (dus met rechtstreekse werking) die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert. Het doel is niet alleen om de bescherming van persoonsgegevens binnen de Europese Unie te garanderen, maar ook om het vrije verkeer van gegevens binnen de Europese interne markt te waarborgen.
Betrokkene	De geïdentificeerde of identificeerbare persoon van wie zijn of haar gegevens worden verwerkt.
Covid Safe Ticket (CST)	Het resultaat van de lezing van het digitaal EU-COVID-certificaat middels de applicatie bedoeld in artikel 17 van Samenwerkingsakkoord van 14 juli 2021 (gewijzigd op 27 september 2021)tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVID-certificaat, het COVID Safe Ticket, het PLF en de verwerking van persoonsgegevens van in het buitenland wonende of verblijvende werknemers en zelfstandigen die activiteiten uitvoeren in België teneinde de toegang tot een proef- en pilootproject, massa-evenement, dancings en discotheken of aangelegenheden en voorzieningen waarvoor het gebruik van het COVID Safe Ticket kan worden ingezet in de context van de coronavirus COVID-19-pandemie te regelen
De EU-verordening inzake digitale COVID-certificaten	Verordening (EU) 2021/953 van het Europees Parlement en de Raad van 14 juni 2021 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 faciliteren. De EU-verordening inzake digitale COVID-certificaten is op 1 juli 2021 in werking getreden. EU-burgers en -ingezetenen kunnen nu hun digitale COVID-certificaten laten uitgeven en verifiëren in de hele EU.
Digitaal Europees Covid Certificaat DEUCC	Certificaat zoals bedoeld in de EU-verordening inzake digitale COVID-certificaten

Gegevensbeschermings-effectbeoordeling (GEB)	Indien een gegevensverwerking waarschijnlijk gepaard gaat met hoge risico's in verband met de rechten en vrijheden van natuurlijke personen, is de verwerkingsverantwoordelijke of de verwerker verantwoordelijk voor het verrichten van een gegevensbeschermingseffectbeoordeling om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren. Met het resultaat van de beoordeling dient rekening te worden gehouden bij het bepalen van de passende maatregelen die moeten worden genomen om aan te tonen dat de AVG bij de verwerking van persoonsgegevens wordt nageleefd.
Gegevens over gezondheid	Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, inclusief gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.
Inbreuk in verband met persoonsgegevens/datalek/gegevenslek	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
INSZ nummer	Identificatie Nummer voor de Sociale Zekerheid.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); 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 identificatienummer, 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.
Pseudonimiseren van gegevens	Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Samenwerkingsakkoord betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVID-certificaat en het COVID Safe Ticket.	Samenwerkingsakkoord tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVID-certificaat, het COVID Safe Ticket, het PLF en de verwerking van persoonsgegevens van in het buitenland wonende of verblijvende werknemers en zelfstandigen die activiteiten uitvoeren in België.Dit betreft zowel het samenwerkingsakkoord van 14 juli 2021 met aanvulling van 27 september 2021 als het uitvoerend samenwerkingsakkoord van 27 september 2021.
Suspension list Lijst met ID's van certificaten die tijdelijk geschorst zijn	Betreft een lijst met ID's van certificaten die tijdelijk geschorst zijn; identifiers van certificaten (DEUCC) die tijdelijk niet de mogelijkheid bieden om een CST te valideren.
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
Verwerkingsverantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

Algemene toelichting

Op 11 maart 2020 heeft de Wereldgezondheidsorganisatie (WGO) de uitbraak van het SARS-CoV-2-virus, dat de ziekte COVID-19 veroorzaakt, uitgeroepen tot een pandemie.

Ook België blijft niet gespaard van deze pandemie. In het kader van de COVID-19-gezondheidscrisis en om een verdere verspreiding van het SARS-CoV-2-virus (hierna "coronavirus COVID-19") tegen te gaan, werd de Nationale Veiligheidsraad, waarin naast de vertegenwoordigers van de federale overheid, vertegenwoordigers van de gefedereerde entiteiten zetelen, belast om op elkaar

afgestemde maatregelen te nemen teneinde de verdere verspreiding van het coronavirus COVID-19 te beperken.

Niettegenstaande het essentieel is de verdere verspreiding van het coronavirus COVID-19 te beperken, moet eveneens rekening worden gehouden met de heropstart van de activiteiten van de burgers zoals deze werden uitgeoefend voor de COVID-19- pandemie, waaronder de mogelijkheid om te reizen binnen de Europese Unie en culturele en andere evenementen en activiteiten te bij te wonen. Eveneens moet volop ingezet worden op het herstel na de COVID-19-pandemie.

Aangezien een uniforme regelgeving omtrent de vrijheid voor EU-burgers om te reizen en te verblijven op het grondgebied van de lidstaten, aangewezen is, heeft de Europese Unie voorzien in een wetgevend kader, bestaande uit enerzijds de Verordening (EU) 2021/953 van 14 juni 2021 van het Europees Parlement en de Raad betreffende een kader voor de afgifte, verificatie en aanvaarding van interoperabele COVID19-vaccinatie-, test- en herstelcertificaten (digitaal EU-COVID-certificaat) teneinde het vrije verkeer tijdens de COVID-19-pandemie te faciliteren ("Verordening digitaal EU COVID-certificaat") en de Verordening (EU) 2021/954 van het Europees Parlement en de Raad van 14 juni 2021 betreffende een kader voor de afgifte, verificatie en aanvaarding van interoperabele COVID19-vaccinatie-, test- en herstelcertificaten (digitaal EU-COVID-certificaat) ten aanzien van onderdanen van derde landen die legaal op het grondgebied van de lidstaten verblijven of wonen tijdens de COVID-19-pandemie ("Verordening digitaal EU COVID-certificaat voor onderdanen derde landen").

De Verordening digitaal EU-COVID-certificaat laat tevens verder binnenlands gebruik van het digitaal EU-COVID-certificaat toe, voor zover dit binnenlands gebruik gestoeld is op een wettelijke basis. Een samenwerkingsakkoord[1] bepaalt onder andere deze wettelijke basis.

Conform de notificaties van het Overlegcomité 11 mei en 4 juni 2021 werd beslist om vanaf de inwerkingtreding van dit samenwerkingsakkoord, de toegang tot proef- en pilootprojecten en vanaf 13 augustus 2021 de toegang tot massa-evenementen te regelen op grond van het COVID Safe Ticket.

Het COVID Safe Ticket is het resultaat van de lezing van het digitaal EU-COVIDcertificaat middels de COVIDScan-applicatie teneinde de toegang tot een proef- en pilootproject of massa-evenement dancings en discotheken of aangelegenheden en voorzieningen waarvoor het gebruik van het COVID Safe Ticket kan worden ingezet in de context van de COVID-19-pandemie te regelen. Het COVID Safe Ticket maakt aldus het binnenlands gebruik van het digitaal EU-COVID-certificaat mogelijk.

Teneinde het digitaal EU-COVID-certificaat op een gebruiksvriendelijke en toegankelijke wijze ter beschikking te stellen aan de burgers, worden (minstens) twee applicaties ontwikkeld, met name de COVIDSafe-applicatie en de COVIDScan-applicatie. De COVIDSafe-applicatie heeft als doel de houder van het digitaal EU-COVID-certificaat toe te laten dit op te vragen en de streepjescode te laten inscannen. Ook kan men desgevallend het COVID Safe Ticket op de COVIDSafe-application genereren. De COVIDScan-applicatie laat toe om via het scannen van de streepjescode van het digitaal EU-COVID-certificaat de echtheid en geldigheid van het digitaal EU-COVID-certificaat te

[1]" [14.07.2021] Samenwerkingsakkoord tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVID-certificaat, het COVID Safe Ticket, het PLF en de verwerking van persoonsgegevens van in het buitenland wonende of verblijvende werknemers en zelfstandigen die activiteiten uitvoeren in België" en de daaropvolgende relevante samewerkingsakkoorden

valideren en desgevallend het COVID Safe Ticket te genereren. Deze streepjescode kan ook een tweedimensionale streepjescode, met name een QR-code, uitmaken.

De COVIDSafe-applicatie wordt vanaf 16 juni 2021 ter beschikking gesteld aan de burgers en kan vanaf 1 juli 2021 gebruikt worden voor het reizen binnen de Europese Unie.

Vanaf de inwerkingtreding van het samenwerkingsakkoord, kan het COVID Safe Ticket via de COVIDScan-applicatie of desgevallend via de COVIDSafe-applicatie gegenereerd worden voor binnenlands gebruik, meer bepaald voor proef- of pilootprojecten dancings en discotheken of aangelegenheden en voorzieningen waarvoor het gebruik van het COVID Safe Ticket kan worden ingezet in de context van de coronavirus COVID-19-pandemie vanaf de inwerkingtreding van dit samenwerkingsakkoord, en voor massa-evenementen vanaf 13 augustus 2021 die worden georganiseerd in het geldende besluit houdende de maatregelen van bestuurlijke politie om de verspreiding van het coronavirus COVID-19 te beperken.

Sectie I: Identificatie van de nood van een gegevensbeschermings-effectbeoordeling

De verwerking van gegevens met betrekking tot het digitaal EU-COVID-certificaat en het COVID Safe Ticket betreft een verwerking van persoonsgegevens.

Gelet op

- artikel 35 van de AVG, en
- de richtsnoeren van de Groep Gegevensbescherming Artikel 29 voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679 wordt er geoordeeld dat de gegevensverwerkingen met betrekking tot het digitaal EU-COVID-certificaat en het COVID Safe Ticket een GEB vereist.

Het besluit tot noodzaak van een GEB is in het bijzonder gebaseerd op volgende elementen:

- De verwerking betreft een grootschalige verwerking van een bijzondere categorie van persoonsgegevens, met name gezondheidsgegevens. Het gaat daarbij over gegevens gerelateerd aan vaccinatie, resultaten van testen op COVID besmettingen en herstel na besmetting.
- CST betreft alle personen ouder dan 12 jaar. Het gaat dus ook over kwetsbare personen zoals kinderen (vanaf 13 jaar), werknemers, geesteszieken, asielzoekers, bejaarden,...

Deze GEB heeft geen betrekking op de gegevensverwerkingen betreffende het registreren van vaccinaties, het verwerken van de resultaten van testen of het registreren van het herstel van een betrokkene van een COVID infectie. Deze GEB beperkt zich tot het valideren van een digitaal EU-COVID certificaat en desgewenst het genereren van CST vanaf het digitaal EU-COVID certificaat.

Sectie II: Beschrijving van de gegevensverwerkingen

Verwerkingen

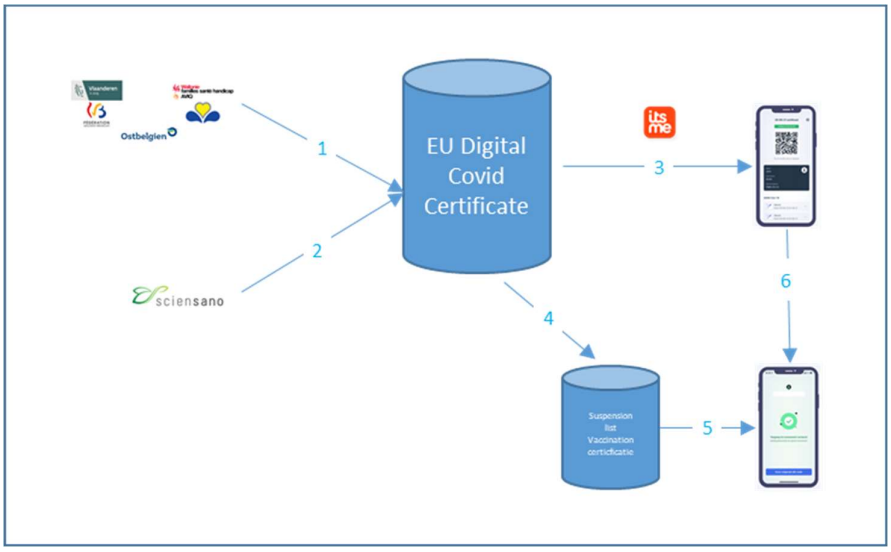
De COVIDScan app heeft 2 mogelijke verwerkingen:

1. Inkomende reiziger : de COVIDScan app zal de gegevens van de QR code inlezen en valideren of de houder van het certificaat voldoet aan de voorwaarden bepaald in de validatieregels.

Er worden geen andere persoonsgegevens verwerkt dan degene die aangereikt zijn door de aanbieder van de certificaat.

2. CST module : de COVIDScan app zal gegevens van de QR code inlezen en valideren of de houder van het certificaat voldoet aan de voorwaarden bepaald in de validatieregels en of het certificaat tijdelijk of permanent geschorst is.

De verwerkingen in het kader van CST kunnen als volgt voorgesteld worden:



1. De aangeduide instellingen van de verschillende regio's voeden, via het platform Vaccinnet, het centrale platform met de vaccinatiecertificaten.
2. Sciensano voedt het centrale platform met de informatie betreffende herstelcertificaten en resultaten van PCR testen
3. De burger kan zijn relevante certificaten downloaden. Dit gebeurt door middel van de toepassing CovidSafe maar de certificaten kunnen ook beschikbaar gesteld worden op andere dragers zoals papier. De burger dient hiervoor te authentiseren met behulp van een authenticatiemiddel vanaf niveau FAS 350.
4. Vanuit het centrale platform wordt een lijst opgesteld met certificaten die tijdelijk geschorst worden omdat de houder van het certificaat een positieve COVID test heeft afgelegd of omdat het certificaat door de houder of uitgever werd ingetrokken. Deze lijst wordt op uurbasis geüpdated en bevat enkel de identifiers van de geschorste certificaten. Geen enkele andere identifier die het mogelijk maakt de houder van het certificaat te identificeren zal in deze lijst voorkomen.
5. De lijst met identifiers van certificaten die geschorst zijn, wordt op regelmatige basis naar de app "CovidScan" getransfereerd.
6. Wanneer een burger, om toegang te verkrijgen, een CST dient te bekomen, dan zal deze zijn DEUCC vertonen die door de CovidScan app zal worden ingelezen waarna de CovidScan app zal nagaan of de ID van de DEUCC in de lijst van geschorste certificaten voorkomt. Indien dit het geval is, dan zal het CST niet gecreëerd worden en een rood signaal geven. In het andere geval zal de CovidScan app een groen signaal geven voor zover dat het vertoonde DEUCC een geldig certificaat is.

Persoonsgegevens

De gegevens die worden verwerkt zijn vastgelegd in het voornoemde samenwerkingsakkoord.

Voor het afleiden van COVID Safe Ticket worden de categorieën persoonsgegevens van het digitaal EU-COVID-certificaat verwerkt.

Het COVID Safe Ticket

Het COVID Safe Ticket bevat en geeft slechts volgende gegevens weer:

- de aanduiding of de houder, in zijn hoedanigheid van bezoeker van een massa-evenement, een proef- en pilootproject, een dancing of discotheek of aangelegenheden en voorzieningen waarvoor het gebruik van het COVID Safe Ticket kan worden ingezet, de toegang tot het massa-evenement, proef- en pilootproject, dancing of discotheek of de aangelegenheden en voorzieningen waarvoor het gebruik van het COVID Safe Ticket kan worden ingezet mag worden toegestaan of dient te worden geweigerd
- identiteitsgegevens van de houder, namelijk de naam en voornaam
- geldigheidsduur van het COVID Safe Ticket.

Het digitaal EU-COVID-certificaat

De gegevens die worden verwerkt in het digitaal EU-COVID-certificaat zijn vastgelegd in de VERORDENING (EU) 2021/953 VAN HET EUROPEES PARLEMENT EN DE RAAD van 14 juni 2021 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[2].

In het vaccinatiecertificaat op te nemen gegevensvelden:

a)naam: familienaam of familienamen en voornaam of voornamen (in die volgorde);

b)geboortedatum;

c)doelziekte of -ziekteverwekker: COVID-19 (SARS-CoV-2 of een van de varianten ervan);

d)COVID-19-vaccin of -profylaxe;

e)productnaam van het COVID-19-vaccin;

f)handelsvergunninghouder of producent van het COVID-19-vaccin;

g)volgnummer in een reeks doses alsook totale aantal doses in de reeks;

h)datum van vaccinatie, met vermelding van de datum van de laatste ontvangen dosis;

i)lidstaat of derde land waar het vaccin werd toegediend;

j)afgever van het certificaat;

k)unieke certificaatidentificatiecode.

In het testcertificaat op te nemen gegevensvelden:

a)naam: familienaam of familienamen en voornaam of voornamen (in die volgorde);

[2] Zie link : https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32021R0953

b)geboortedatum;

c)doelziekte of -ziekteverwekker: COVID-19 (SARS-CoV-2 of een van de varianten ervan);

d)type test;

e)benaming van de test (facultatief voor NAAT-test);

f)producent van de test (facultatief voor NAAT-test);

g)datum en tijdstip van de monsterneming;

h)resultaat van de test;

i)testcentrum of -faciliteit (facultatief voor snelle antigeentest);

j)lidstaat of derde land waar de test werd afgenomen;

k)afgever van het certificaat;

l)unieke certificaatidentificatiecode.

In het herstelcertificaat op te nemen gegevensvelden:

a)naam: familienaam of familienamen en voornaam of voornamen (in die volgorde);

b)geboortedatum;

c)ziekte of ziekteverwekker waarvan de houder is hersteld: COVID-19 (SARS-CoV-2 of een van de varianten ervan);

d)datum van het eerste positieve NAAT-testresultaat van de houder;

e)lidstaat of derde land waar de test werd afgenomen;

f)afgever van het certificaat;

g)certificaat geldig vanaf;

h)certificaat geldig tot (ten hoogste 180 dagen na de datum van het eerste positieve NAAT-testresultaat);

i)unieke certificaatidentificatiecode.

Betrokken partijen

Sciensano

Sciensano, sui generis openbare instelling met rechtspersoonlijkheid ingeschreven in de Kruispuntbank van Ondernemingen onder het nummer 0693.876.830, met maatschappelijke zetel in de Juliette Wytsmanstraat 14 te 1050 Elsene. Sciensano is een openbare instelling die voor verschillende beleidsniveaus opdrachten ter ondersteuning van het gezondheidsbeleid uitvoert. Deze opdrachten hebben onder andere betrekking op wetenschappelijk onderzoek, expertadvies en risicobeheer. In het kader van deze opdrachten heeft zij ervaring met het toepassen van gegevensbeschermingsprincipes op vlak van gezondheidsgegevens en het implementeren van methoden van beveiliging en pseudonimisering van gegevens

Artikel 2, § 4, van het samenwerkingsakkoord van 25 augustus 2020 tussen de Federale staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde gefedereerde entiteiten of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano, bepaalt dat Sciensano de verwerkingsverantwoordelijke is van de Gegevensbank I, vermeld in artikel 6 van dit samenwerkingsakkoord.

Sciensano is verantwoordelijk voor de afgifte van de test- en herstelcertificaten, vermeld in artikel 3, § 1, 2° en 3°, van het Samenwerkingsakkoord tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVID-certificaat, het COVID Safe Ticket, het PLF en de verwerking van persoonsgegevens van in het buitenland wonende of verblijvende werknemers en zelfstandigen die activiteiten uitvoeren in België. Ingevolge artikel 15, § 1, van dit samenwerkingsakkoord is Sciensano de verwerkingsverantwoordelijke voor de gegevensverwerkingen in het kader van de test- en herstelcertificaten.

(Gezondheids)administraties van de deelstaten

Artikel 7 van het voornoemd samenwerkingsakkoord van 12 maart 2021 bepaalt dat de bevoegde gefedereerde entiteiten of de door de bevoegde gefedereerde entiteiten aangeduide agentschappen, en de federale overheid, ieder voor hun bevoegdheid, optreden als verwerkingsverantwoordelijke voor de verwerking van de persoonsgegevens bedoeld in voornoemd samenwerkingsakkoord.
Het gaat meer bepaald over de volgende entiteiten of agentschappen:

- voor de personen waarvoor de Vlaamse Gemeenschap bevoegd is: het Agentschap Zorg en Gezondheid;
- voor de personen waarvoor de Franse Gemeenschap bevoegd is: l'Office de la Naissance et de l'Enfance;
- voor de personen waarvoor het Waals Gewest bevoegd is: l'Agence wallonne de la santé, de la protection sociale, du handicap et des familles;
- voor de personen waarvoor de Gemeenschappelijke Gemeenschapscommissie van Brussel-Hoofdstad bevoegd is: de Gemeenschappelijke Gemeenschapscommissie;
- voor de personen waarvoor de Franse Gemeenschapscommissie van Brussel-Hoofdstad bevoegd is: de Franse Gemeenschapscommissie;
- voor de personen waarvoor de Duitstalige Gemeenschap bevoegd is: Ministerium der Deutschsprachigen Gemeinschaft;

De betrokken administraties van de deelstaten zijn:

- Vlaams Agentschap Zorg en Gezondheid (VAZG), ingeschreven in de Kruispuntbank van Ondernemingen onder het nummer 0316.380.841, waarvan de kantoren gelegen zijn Koning Albert II laan 35, bus 33.
- Agence Wallonne pour une Vie de Qualité (AVIQ), ingeschreven in de Kruispuntbank van Ondernemingen onder het nummer 0646.877.855, waarvan de kantoren gelegen zijn Rue de la Rivelaine 21, 6061 Charleroi.

- De Gemeenschappelijke Gemeenschapscommissie (GGC), ingeschreven in de Kruispuntbank van Ondernemingen onder het nummer 0240.682.833, waarvan de kantoren gelegen zijn in de Belliardstraat 71, bus 1, 1040 Brussel.
- Het Ministerium der Deutschsprachigen Gemeinschaft (MDG), ingeschreven in de Kruispuntbank van Ondernemingen onder het nummer 0332.582.613, waarvan de kantoren gelegen zijn in de Gospertstrasse 1, 4700 Eupen.

Onderaannemers

Voor de operationele uitvoering van de voornoemde verordening door de instanties die verantwoordelijk zijn voor de afgifte van de respectieve certificaten, wordt beroep gedaan op het agentschap Digitaal Vlaanderen, opgericht bij besluit van de Vlaamse Regering van 18 maart 2016 houdende de oprichting van het intern verzelfstandigd agentschap Digitaal Vlaanderen en de vaststelling van de werking, het beheer en de boekhouding van het Eigen Vermogen Digitaal Vlaanderen. Dat agentschap staat in voor de aanmaak en de terbeschikkingstelling van de betreffende certificaten en de ontwikkeling van een app overeenkomstig de modaliteiten die in de voornoemde verordening zijn vastgelegd. Zodoende gebeurt de afgifte van alle certificaten op operationeel niveau via eenzelfde systeem.
Aangezien de certificaten onmiddellijk moeten kunnen worden uitgereikt, hebben alle betreffende instanties, verantwoordelijk voor de afgifte van certificaten, beslist beroep te doen op het agentschap Digitaal Vlaanderen.
Dit betekent echter niet dat het agentschap Digitaal Vlaanderen beslist over welke toepassing ter beschikking wordt gesteld aan de burger, noch over de modaliteiten en het tijdstip van de-activering van de COVIDSafe en COVIDScan-applicatie. Het agentschap Digitaal Vlaanderen handelt enkel op instructies van het e-Health-platform en treedt op als verwerker.
Er wordt tevens voorzien in een opdracht aan het agentschap Digitaal Vlaanderen om de betrokkene inzage en toegang te geven tot de officiële versie van zijn vaccinatie- en testgegevens in afwachting van de inwerkingtreding van de Verordening digitaal EU-COVID-certificaat.
Voor de terbeschikkingstelling van de Suspension list wordt gebruik gemaakt van Amazon Web Services.

Organisator van evenementen of uitbater van een zaak waarbij de toegang voor klanten en deelnemers gebeurt onder voorwaarde van vertoon van een geldig CST – Controle op inkomende reizigers

De organisator en uitbater van een zaak die CST dienen te controleren, en de organisatie die inkomende reizigers dient te controleren zijn verwerkingsverantwoordelijken voor het aanmaken van een CST middels de CovidScan app.

Zij dienen als verwerkingsverantwoordelijke de nodige maatregelen te nemen om de app gepast te beschermen en de voorwaarden voor het gebruik van deze app te respecteren. Hieronder vallen ook de beperkingen van bewaartermijnen van gegevens noodzakelijk voor de correcte verwerking van het CST en de resultaten van een controle van DEUCC

Voor elke andere verwerking dan de controle of aanmaak CST met CovidScan door een organisatie of bedrijf die daar een wettelijke reden of verplichting toe heeft, die gebeurt met de gegevens van CST, bestaat geen wettelijke basis.

Houder van een certificaat

De houder van een certificaat zal dit certificaat vertonen om toegang te verkrijgen. De houder van het certificaat wordt geacht de gegevens die op de certificaten, in het bijzonder het ID van het certificaat, niet nodeloos openbaar te maken.

Verwerkingsdoeleinden

Zoals bepaald in Samenwerkingsakkoord tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVID-certificaat, het COVID Safe Ticket, het PLF, en de verwerking van persoonsgegevens van in het buitenland wonende of verblijvende werknemers en zelfstandigen die activiteiten uitvoeren in België :

Het COVID Safe Ticket is het resultaat van de lezing van het DEUCC middels de COVIDScan-applicatie teneinde de toegang tot een proef- en pilootproject, massa-evenement, dancings en discotheken of aangelegenheden en voorzieningen waarvoor het gebruik van het COVID Safe Ticket kan worden ingezet in de context van de coronavirus COVID-19-pandemie te regelen.

Het COVID Safe Ticket maakt aldus het binnenlands gebruik van het digitaal EU-COVID-certificaat mogelijk

Belangen bij de gegevensverwerkingen

De belangen van de betrokken personen, organisatoren van evenementen en uitbaters van bv. horeca zaken situeren zich op volgende vlakken

- vertrouwen door de burger dat de evenementen plaatsvinden in Covid-veilige omstandigheden en zonder dat de afstandsregels, mondmaskers en andere maatregelen dan CST dienen gerespecteerd te worden
- het aanbieden van een kwaliteitsvolle controle door organisatoren van evenementen en uitbaters van bv. horecazaken dat de personen die wensen deel te nemen over een geldig certificaat beschikken.
- een gunstige medische context voor de nagestreefde doeleinden van de gegevensverwerkingen

Vertrouwen bij het brede publiek

De waarde van de certificaten moet correct gepositioneerd worden: het gebruik van de certificaten helpt in eerste instantie de hele maatschappij om op een veilige manier evenementen te organiseren waar meerdere personen kunnen aan deelnemen. Daarnaast vermijdt het CST dat bepaalde voorzieningen (bv. dancings, restaurants, fitnesscentra, …) zouden moeten sluiten.

Kwaliteitseisen

De certificaten en CovidScan applicatie moeten voldoen aan hoge kwaliteitseisen: eenvoudig te installeren en gebruiken, beperkt batterijverbruik om gegevensverwerkingen mogelijk te maken. In het bijzonder moet een certificaat een representatieve inschatting geven over de kans dat de houder van dit certificaat een verspreider van het virus zou kunnen zijn.

Medisch

De data van de labo's , vaccinatiecentra,artsen, … dient betrouwbaar te zijn en verwerkt te worden in de certificaten.

Verwerkingslocaties en conformiteit GDPR

De gegevens met betrekking tot de DEUCC worden verwerkt door Digitaal Vlaanderen als verwerker voor de verschillende verwerkingsverantwoordelijken. Deze gebeuren conform de GDPR regelgeving.

Er vinden enerzijds verwerkingen op het toestel van de gebruiker plaats (CovidScan) en anderzijds binnen de serverinfrastructuur (Afleveren van de certificaten en opstellen en verdelen van de suspension list).

Technieken en methoden van de gegevensverwerkingen

De toepassing van de gegevensbescherming door ontwerp en door standaardinstellingen, principes van de Algemene Verordening Gegevensbescherming, staat centraal.

Voor de bescherming van de gegevens worden volgende technieken toegepast[3]:

1. **Dataminimalisatie** : bij het ontwerp van het Digitaal Europees COVID-certificaat en de CST wordt aandacht besteed aan het minimaliseren van de gegevens die op de certificaten voorkomen zodat enkel de gegevens vermeld in de Europese verordeningen voorkomen. Voor CST wordt de informatie beperkt tot de gegevens zoals vermeld in het relevante samenwerkingsakkoord. Verder wordt ook in de suspension list van de certificaten enkel de ID's van de certificaten vermeld zodat deze certificaten niet kunnen teruggebracht worden tot de houder van dit certificaat. Dit houdt wel in dat de verwerker de nodige maatregelen moet treffen zodat er geen lijsten ter beschikking komen die de ID van de certificaten linkt met de houder van het certificaat.
2. **Bescherming van de integriteit** : de houder van een certificaat kan nadeel ondervinden wanneer de integriteit van de suspension list niet gegarandeerd is. Om dit te voorkomen wordt deze lijst beveiligd met de private sleutel van de uitgever van de lijst
3. **Toegangscontrole substantial voor het bekomen van het certificaat op elektronische wijze**: de certificaten bevatten bepaalde gegevens met betrekking tot de gezondheid. Om die reden wordt de toegang tot de certificaten waar medische informatie op vermeld staat beheerd met FAS niveau 350 of hoger wat door de federale overheidsdienst als een authenticatiemiddel van niveau "substantial" of "High" wordt ingeschaald.
4. **Bescherming van de gegevens in de suspension list door hashing met salting :** dit beperkt de mogelijkheid tot het consulteren van de ID's in de lijst wanneer men wel over het ID beschikt maar niet over de salt (secret)
5. **Bescherming van de lijst door encryptie :** de lijst is niet toegankelijk wanneer men niet over de key beschikt. Deze key wordt ook regelmatig aangepast.
6. **Bescherming van de secrets door obfuscatie van de informatie**: hierdoor wordt het voor aanvallers moeilijk gemaakt om de secrets te bekomen en aldus de informatie in de suspension list te consulteren

[3] Omwille van veiligheidsredenen worden niet alle beveiligingstechnieken vermeld. Deze worden wel meegenomen in de evaluatie van de risico's.

Wanneer een CST gecreëerd wordt door een gebruiker van de CovidScan app, dan dient deze zich te beroepen op de lijst van certificaten die geschorst zijn op het moment dat het DEUCC aangeboden wordt. Deze lijst en zijn inhoud dient publiek te zijn en enkel de ID's van de geschorste certificaten te bevatten, die niet naar een geïdentificeerde persoon verwijzen.

Het is personen strikt verboden om het COVID Safe Ticket te genereren en in te lezen voor andere doeleinden dan deze gestipuleerd in het voornoemde samenwerkingsakkoord van 14 juli 2021 en latere samenwerkingsakkoorden en verordeningen die dit uitbreiden. Personen die het COVID Safe Ticket genereren of inlezen voor doeleinden die niet voorzien zijn, kunnen worden gestraft met gemeenrechtelijke sancties, inclusief strafrechtelijke sancties.

Juridisch & beleidsmatig kader

Het juridisch en beleidsmatig kader speelt zich af op drie beleidsniveaus: Europees, (inter)federaal en deelstatelijk. Hieronder volgt een lijst van de voornaamste regelgeving, aanbevelingen of beleidsinitiatieven.

Europese Unie

- *VERORDENING (EU) 2021/953 VAN HET EUROPEES PARLEMENT EN DE RAAD van 14 juni 2021 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*
- *Verordening (EU) 2021/954 van het Europees Parlement en de Raad van 14 juni 2021 betreffende een kader voor de afgifte, verificatie en aanvaarding van interoperabele COVID-19-vaccinatie-, test- en herstelcertificaten (digitaal EU-COVID-certificaat) ten aanzien van onderdanen van derde landen die legaal op het grondgebied van de lidstaten verblijven of wonen tijdens de COVID-19-pandemie*

Federaal en interfederaal

- *Samenwerkingsakkoord van 12 maart 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot vaccinaties tegen COVID-19*
- *Samenwerkingsakkoord van 11 juni 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de operationalisering van de Verordening (EU) 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 (EU Digitaal COVID Certificaat)*
- *Samenwerkingsakkoord van 14 juli 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVIDcertificaat, het Covid Safe Ticket, het PLF en de verwerking van persoonsgegevens van in het buitenland wonende of verblijvende werknemers en zelfstandigen die activiteiten uitvoeren in België*

- *Samenwerkingsakkoord van 27 september 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVIDcertificaat, het Covid Safe Ticket, het PLF en de verwerking van persoonsgegevens van in het buitenland wonende of verblijvende werknemers en zelfstandigen die activiteiten uitvoeren in België*
- *Uitvoerend samenwerkingsakkoord van 15 oktober 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVID-certificaat, het COVID Safe Ticket, het PLF en de verwerking van persoonsgegevens van in het buitenland wonende of verblijvende werknemers en zelfstandigen die activiteiten uitvoeren in België*
- *Uitvoerend samenwerkingsakkoord van 27 september 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVID-certificaat, het Covid Safe Ticket, het PLF en de verwerking van persoonsgegevens van in het buitenland wonende of verblijvende werknemers en zelfstandigen die activiteiten uitvoeren in België*
- *Samenwerkingsakkoord van 25 augustus 2020 tussen de Federale staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie, betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde gefedereerde entiteiten of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano*

Bewaartermijnen

De bewaartermijnen van de persoonsgegevens die worden verwerkt ten behoeve van het DEUCC, worden strikt begrensd tot het doel van het DEUCC of tot wanneer het DEUCC niet langer gebruikt mag worden om het recht van vrij verkeer uit te oefenen, zoals bepaald door de Verordening digitaal EU-COVID-certificaat.

De certificaten worden op het toestel van de houder van het certificaat bewaard zolang deze geldig zijn en worden verwijderd wanneer de gebruiker de app van zijn toestel verwijdert. (CovidSafe)

Er worden geen gegevens bewaard op de CovidScan app anders dan de Suspension list.

Sectie III: Beoordeling noodzakelijkheid & proportionaliteit

Rechtmatigheid van de verwerking

De vermelde verwerkingen in deze GEB zijn rechtmatig omdat deze verwerkingen gebaseerd zijn op redenen van algemeen belang. (art. 6, 1, e) GDPR) en op de wettelijke verplichting die op de organisator of uitbater van een zaak rust en die de toegang pas mag toestaan wanneer een geldig CST

werd gegenereerd. De verwerkingsactiviteiten hebben namelijk als oogmerk om de verspreiding van COVID-19 in te dijken en de bevolking tegen deze epidemie te beschermen. De gegevensverwerkingen zijn geregeld via de wettelijke kaders vervat in de samenwerkingsakkoorden en de Europese verordeningen.

Bijzondere persoonsgegevens

Het verbod op de verwerking van gezondheidsgegevens is voor deze verwerkingen niet van toepassing aangezien de doelstellingen gelinkt zijn aan de vervulling van een taak van algemeen belang op het gebied van de volksgezondheid zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid (art. 9 § 2 i) GDPR).

Doelbinding

De verwerkingen van persoonsgegevens voor het aanbieden van CST beperken zich tot de verwerkingen zoals omschreven in het voornoemde samenwerkingsakkoord van 14 juli 2021.

Er worden geen andere verwerkingen toegestaan met de verkregen persoonsgegevens en certificaten bij het creëren van het CST.

4.4. Noodzaak en evenredigheid

Het gebruik van CST is voorzien om toegang te verlenen tot een evenement of een gebouw waar diensten zoals horeca of fitness worden verleend[4]. De reglementen voor dit gebruik worden bepaald op federaal, regionaal of gemeentelijk niveau. Enig ander gebruik van CST is niet toegestaan.
Om dit te faciliteren werd de CovidScan App ontwikkeld en ter beschikking gesteld van de organisaties die toegangscontrole dienen uit te voeren.
Om de controle te kunnen uitvoeren zal de CovidScan gebruik maken van de validatieregels die gedownload worden en bijkomend voor het afleiden van de CST van de informatie in de “Suspension list”. Omdat de app de controle “offline” moet kunnen uitvoeren dient de suspension list gedownload te worden door de app en lokaal bewaard te zijn. Om aan de vereiste van offline controle te kunnen voldoen is dit een noodzaak en een evenredige maatregel.
Wanneer een controle wordt uitgevoerd, kan CovidScan de gegevens van de QR code uitlezen. Deze gegevens worden niet door de app bewaard. Vanwege de doelstelling, het controleren van de geldigheid van de vertoonde certificaten, is deze verwerking noodzakelijk. Door de beperking van de verwerkte gegevens voor de controle inkomende reiziger en het aanmaken van een CST is dit ook evenredig.

4.5. Rechten van de betrokkenen

Onder de voorwaarden van de AVG hebben gebruikers het recht om toegang te krijgen tot hun persoonsgegevens, om rectificatie, uitwissing of beperking van de verwerking te verzoeken of om bezwaar te maken tegen de verwerking van hun persoonsgegevens ("rechten van de betrokkene").

De betrokkene zal zijn certificaten bekomen met gebruik van de CovidSafe app, downloaden via daartoe bestemde sites of verkrijgen op papier na aanvraag bij de bevoegde overheden. De rechten van betrokkenen voor wat betreft de toegang, rectificatie, beperking van de verwerking of bezwaar

[4] Deze lijst wordt dynamisch bepaald door de federale overheid, de gefedereerde entiteiten en lokale besturen.

tegen de verwerking van hun gegevens kunnen uitgeoefend worden bij de daartoe bevoegde overheden zoals vermeld in de privacyverklaring van deze certificaten op www.covidsafe.be.

Bij de creatie van de CST door de CovidScan app wordt gebruik gemaakt van de “Suspension list”. Een betrokkene die zijn rechten wilt uitoefenen betreffende deze suspension list kan hiervoor contact opnemen met de verwerkingsverantwoordelijke voor het getoonde certificaat. Deze zal de vraag behandelen in zoverre deze niet conflicteren met de wettelijke voorwaarden die de bruikbaarheid van het certificaat voor het afleiden van CST vastleggen.

Sectie V: Informatieveiligheid

Het gebruik van het COVID Safe Ticket voorziet dat de houder van een DEUCC kan aantonen dat hij/zij over een geldig certificaat beschikt om toegang te verkrijgen tot een evenement of een inrichting die de verplichting heeft dit te controleren. Om misbruiken te voorkomen dient de organisatie van het evenement of de inrichting te kunnen nagaan of de houder van het gecontroleerde certificaat en degene die het presenteert om toegang te verkrijgen dezelfde zijn. Om die reden is het niet mogelijk noch wenselijk het certificaat te anonimiseren of volledig te pseudonimiseren.

Dit betekent dat de verwerkingen voor het creëren van CST zodanig moeten ingericht worden dat de informatie die gedeeld wordt:

- De minimale informatie is die nuttig is voor het creëren van CST
- De publiek gedeelde informatie niet kan teruggebracht worden tot de betrokkenen
- De betrokkene zelf de sleutel in handen heeft om enkel de relevante delen van de publiek gedeelde informatie tot zichzelf terug te brengen

Naast de confidentialiteit is het ook belangrijk de integriteit van de verwerkte gegevens te garanderen. Immers, wanneer het CST niet op basis van correcte informatie wordt gecreëerd, kan een betrokkene ten onrechte toegang worden geweigerd of onterecht toegang worden verleend waarbij in dit laatste geval de gezondheid van andere bezoekers in gevaar wordt gebracht.

Deze GEB behandelt enkel de afleiding van het CST en de controle op inkomende reiziger vanaf de DEUCC waarbij ervan wordt uitgegaan dat het risico van inbreuken op confidentialiteit en integriteit bij de verwerkingen tot het terbeschikking stellen van het certificaat aan de burger reeds in andere GEB’s werd opgenomen.

Deze GEB behandelt enkel de afleiding van het CST en de controle op inkomende reiziger vanaf de QR code van een DEUCC. Het behandelt dus niet de risico’s eigen aan het bekomen van DEUCC op papier, door downloaden of door het gebruik van CovidSafe.

Minimalisatie van de verwerkte informatie

Deze app zal slechts de minimale informatie verwerken die noodzakelijk is voor het creëren van een CST en bij de controle op inkomende reiziger.

Hiertoe heeft de wetgever reeds een eerste controle ingebouwd door vast te leggen welke informatie mogen verwerkt worden voor het aanmaken van de CST.

Bijkomend zal de CovidScan app enkel het DEUCC scannen en het resultaat van de validatie weergeven op het scherm samen met eenvoudige identificatiegegevens (naamgegevens) om de houder van het certificaat te identificeren. Er zal verder geen informatie bewaard worden op de mobiele toestellen.

Gebruik van de suspension list

De suspension list is een lijst van ID's van DEUCC certificaten. Deze lijst wordt afgeleid van de lijst van uitgegeven certificaten enerzijds en resultaten van PCR & RAT testen en beslissingen tot intrekking van certificaten anderzijds. Deze resultaten zijn opgeslagen in een centrale database waarvoor de verwerkingsverantwoordelijken deze zijn die verantwoordelijk zijn voor de uitgifte van de vaccinatiecertificaten en test- en herstel-certificaten. De gegevens in deze database zijn gekoppeld via het INSZ nummer van de betrokkenen en dient daarom als strikt confidentieel beschouwd te worden.

Het doel van de suspension list is het nagaan of een certificaat al dan niet geschorst is omdat er een positief resultaat op een erkende COVID besmettingstest van de betrokkene werd afgeleverd of omdat het certificaat ingetrokken werd. De suspension list bestaat uit enkel ID's van certificaten die op het moment van de uitgifte van de suspension list geschorst zijn.

De ID's van deze certificaten zijn totaal willekeurig bepaald en zijn niet afgeleid van eigenschappen van de betrokkene. Om die reden kan een ID als een pseudoniem beschouwd worden dat niet tot de betrokkene kan teruggebracht worden zonder over bijkomende informatie te beschikken. Vermits de relatie tussen betrokkene en het ID van het certificaat enkel in de centrale database gemaakt wordt, zal de bescherming voor de betrokkene geboden worden door de bescherming van de gegevens in deze centrale database.

Ondanks dat de ID's reeds als beschermd kunnen beschouwd worden, zal de lijst getekend, geëncrypteerd en de ID's van vaccinatiecertificaten die tijdelijk geschorst zijn bijkomend gehashed op het internet worden aangeboden. Het dient erkend te worden dat dit slechts als een verhoging van de veiligheid kan beschouwd worden. Gezien de verdeling van de lijst dient te gebeuren naar een ongekende en ongecontroleerde groep van gebruikers zullen ook de sleutels om de lijst te decrypteren moeten beschikbaar gemaakt worden en kan nadien via toepassing van de hash gevalideerd worden of een certificaat identificatie nummer voorkomt in de lijst. Deze laatste maatregelen verhogen wel de complexiteit om de lijst te ontcijferen maar sluiten als alleenstaande veiligheidsmaatregel niet voldoende de mogelijkheid uit om na te gaan of een certificaat identificatie nummer voorkomt op de lijst.

Veiligheidsmaatregelen binnen CovidScan app

Binnen de CovidScan app dient de beslissing genomen te worden om, na inlezen van de DEUCC en het valideren van aangeboden certificaten op basis van de suspension list, een CST te creëren. Omdat de informatie in deze lijst door een onbekende groep van gebruikers moet kunnen ingelezen worden, dient de informatie in deze lijst publiek beschikbaar te zijn. Toch zijn er extra voorzieningen getroffen om deze lijst bijkomend te beschermen. Deze maatregelen zijn supplementair aan de reeds bestaande maatregelen om de belangen van de betrokkenen te beschermen.

Die maatregelen die een mogelijk misbruik van de lijst technisch bemoeilijken, en die op heden allemaal in voege zijn, bestaan uit:

- **Tekenen** van de lijst van certificaatcodes ten behoeve van de controle van de echtheid/integriteit van de lijst
    - Wordt getekend op de servers van Digitaal Vlaanderen met Private key
    - Gevalideerd in de COVIDScan-applicatie met Public key
- **Encrypteren** van de volledige lijst van certificaatcodes
    - Door middel van de Public key op de servers van Digitaal Vlaanderen
- **Decrypteren** met Private key die beschermd wordt door de COVIDScan-applicatie
- **Hashing** van de individuele certificaatcodes met salting
- **Obfuscation** (vertroebeling) van de broncode van de COVIDScan-applicatie

- Dit is een techniek die het moeilijk maakt om de broncode van de COVIDScan-applicatie te bekomen door middel van een decompilering van de COVIDScan-applicatie

De "Suspension list" wordt getekend, versleuteld en de ID's in de lijst zijn gehashed voordat deze lijst wordt aangeboden via een s3 bucket. Zowel de salt voor de hash als de encryptiesleutels worden regelmatig vervangen.

Het is duidelijk dat bij het reverse engineeren van de app deze bescherming verdwijnt. Om die reden wordt de obfuscatie van de software toegepast.

Sectie VI: Beschrijving en beoordeling risico's voor de betrokkenen & voorgenomen maatregelen

Voor de inschatting van privacy-risico's gerelateerd aan de gegevensverwerkingen van de CovidScan App maakt deze GEB gebruik van risico-analyse tools van de Kruispuntbank van de Sociale Zekerheid en Tomas Moore.

Onderstaand zijn de risico's gegroepeerd volgens de doelstellingen.

- D01. Naleving van het recht op transparantie van de gegevensverwerking
- D02. Naleving van doelbinding van de gegevensverwerking
- D03. Naleving van dataminimalisatie
- D04. Waarborgen van de kwaliteit van persoonsgegevens
- D05. Naleving van de vereisten inzake opslagbeperking
- D06. Naleving van het recht op bescherming van vertrouwelijkheid en veiligheid van de gegevensverwerking
- D07. Rechtmatigheid van de verwerking van persoonsgegevens
- D08. Naleving van het recht op informatie (over gegevensverwerking)
- D09. Naleving van het recht op verbetering en verwijdering van persoonsgegevens
- D10. Naleving van het recht op overdraagbaarheid van gegevens
- D11. Naleving van het recht op bezwaar
- D12. Naleving van de regeling in verband met geautomatiseerde individuele besluiten
- D13. Naleven van de (technische) verplichtingen inzake opzet van de verwerking
- D14. Naleven van organisatorische verplichtingen

In de risicobeschrijving worden de probabiliteit (onwaarschijnlijk/waarschijnlijk/zeer waarschijnlijk) en de impact (beperkt/middelmatig/groot) van een risico beschreven. Samen vormen ze een algehele risicoscore.

D01. Naleving van het recht op transparantie van de gegevensverwerking

Principe	Vertel de betrokkene welke informatie u verzamelt, wat u daarmee gaat doen en wat de gevolgen zijn van de dataverwerking
Samenvatting	Hoe brengt u de betrokkene op de hoogte van de dataverwerking? Of ligt het zo voor de hand dat u het niet hoeft uit te leggen? Als u niet open bent met hen over wat u doet, welke van de uitzonderingen maakt dat u hierover niet communiceert?
Link AVG	Artikel 5 a) behoorlijk en transparante verwerking

R01. Informering persoonsgegevens

R01. Informering persoonsgegevens	
Kwetsbaarheid	
De betrokkene werd niet/onvolledig/onvoldoende geïnformeerd dat er persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt.	
Toelichting	
AVG vereist dat de gebruiker op eenvoudige wijze wordt geïnformeerd over de verwerkingen van zijn persoonsgegevens. Wanneer de informatie niet eenvoudig beschikbaar is dan kan de gebruiker onwetend zijn informatie beschikbaar stellen.	
Maatregelen	
Opmaak van een beschrijving bij CovidSafe waarbij aangegeven wordt welke informatie wordt verwerkt, wie de verwerkingsverantwoordelijken zijn en waar deze kan gevonden worden. Vermelding van de specifieke website https://covidsafe.be/nl/privacy-gegevens https://covidscan.be/front/pdf/privacy-statement-covidscan-app-v1-nl.pdf De informatie over de wetgeving is ook beschikbaar. Om redenen van leesbaarheid door de burger werd hiernaar niet gerefereerd. De DPIA wordt gepubliceerd op de website www.covidscan.be.	
Residueel risico	
In deze is er laag residueel risico. De verwerkte gegevens zijn duidelijk aangegeven. De doelstelling van de verwerking is in wetgeving opgenomen en opgelegd aan zowel de organisatoren als de deelnemers.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R02. Informering doel gegevensverwerking

R02. Informering doel gegevensverwerking
Kwetsbaarheid
De betrokkene werd niet/onvolledig/onvoldoende geïnformeerd over het doel van de gegevensverwerking.
Toelichting
Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is („rechtmatigheid, behoorlijkheid en transparantie"). De transparantie vereist dat de betrokkene geïnformeerd wordt over alle verwerkingen die met zijn gegevens zullen gebeuren.
Maatregelen
De doelstellingen van de verwerking zijn vastgelegd in het samenwerkingsakkoord van 14 juli 2021. Bijkomend heeft de overheid via verschillende media aangegeven welke doelstellingen beoogd worden bij het gebruik van CST. Dit samenwerkingsakkoord legt ook vast dat deze informatie niet kan gebruikt worden voor enige andere finaliteit. De overheid heeft een app ter beschikking gesteld van organisaties die, om toegang te verlenen, het DEUCC dienen te controleren. Hierdoor worden de verzamelde informatie en verwerkingen beperkt tot wat bij wet is toegestaan. De DPIA wordt gepubliceerd op de website www.covidscan.be.
Residueel risico
Door de beperking bij wet van de finaliteiten en de app is het residuele risico beperkt. Wanneer een derde alsnog informatie van burgers zou verwerken voor een andere finaliteit dan toegang te verlenen wanneer daar de controle daarop een wettelijke verplichting (of optie) toe is, dan loopt

R02. Informering doel gegevensverwerking	
de verwerkingsverantwoordelijke het risico op strafrechtelijke vervolging en kan een klacht door de betrokkene worden ingediend bij de GBA.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	2
Risico	LAAG

R03. Geautomatiseerde beslissingen

R03. Geautomatiseerde beslissingen
Kwetsbaarheid
Het probabilistische algoritme achter de geautomatiseerde beslissingsprocedures is niet of onvoldoende duidelijk waardoor de juistheid van de machine conclusies niet kan worden nagegaan.
Toelichting
De app zal op basis van informatie in het DEUCC, de validatieregel externe lijst een CST afleveren. Indien het beslissingsproces niet duidelijk is gedefinieerd, dan riskeert een betrokkene ten onrechte toegang geweigerd te worden of lopen bezoekers het risico dat alsnog besmet te worden door een derde.
Maatregelen
De overheid heeft in de verschillende samenwerkingsakkoorden de beslissingsboom van.(zie link)[5] de verwerkingen vastgelegd. Het algoritme hiervoor wordt ook in de CST module van CovidSafe app toegepast.
Residueel risico
Wanneer het algoritme niet correct is vastgelegd kan de betrokkene toegang geweigerd worden of ten onrechte toegang verleend worden. Door de publicatie van het algoritme is het duidelijk welke criteria er gehanteerd worden en is de probabiliteit klein. Bijkomend zal de app CovidScan hier bijkomend correcte ondersteuning geven. Hierdoor kan ook de betrokkene nagaan of een DEUCC een grond is voor een CST.
Risicoscore
Probabiliteit na maatregelen	1
Impact na maatregelen	2
Risico	LAAG

D02. Naleving van Doelbinding van de gegevensverwerking

Principe	Gebruik de data voor het doel waarvoor u het hebt verzameld, tenzij er een uitzondering van toepassing is
Samenvatting	Wees duidelijk over het doel van het hebben en gebruiken van de data. Is dit wat de persoon zal verwachten? Gebruikt u het voor een ander doel dan waarvoor u het hebt verzameld? Zo ja, is er een uitzondering die dit gebruik rechtvaardigt?
Link AVG	Artikel 5 b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden

[5] Gezien dit document statisch is, wordt aan de lezer aangeraden de laatste versie van het uitvoerend samenwerkingsakkoord te consulteren. CovidScan zal steeds de relevante beslissingsboom geïmplementeerd hebben.

R04. Gespecificeerd doel

R04. Gespecificeerd doel	
Kwetsbaarheid	
Het doel van de gegevensverwerking is niet gespecificeerd. Het is niet gespecificeerd dat de verzamelde gegevens alleen worden gebruikt voor een specifiek doel of dienst.	
Toelichting	
Het soort en de hoeveelheid persoonsgegevens die een onderneming/organisatie mag verwerken, hangt af van de redenen voor de verwerking (gebruikte juridische reden) en het beoogde gebruik van de persoonsgegevens. De onderneming/organisatie moet verschillende belangrijke regels eerbiedigen, waaronder: • persoonsgegevens moeten op een wettige en transparante manier worden verwerkt, waarbij billijkheid ten opzichte van de personen van wie persoonsgegevens worden verwerkt, moet worden gewaarborgd („wettelijkheid, billijkheid en transparantie"); • er moeten specifieke doeleinden zijn voor de verwerking van de gegevens en de onderneming/organisatie moet die doeleinden duidelijk maken aan de personen van wie de persoonsgegevens worden verzameld. Een onderneming/organisatie mag niet zomaar persoonsgegevens verzamelen voor ongedefinieerde doeleinden („doelbinding"); • de onderneming/organisatie mag alleen de persoonsgegevens verzamelen en verwerken die nodig zijn om dat doel te bereiken	
Maatregelen	

Het CST steunt op verschillende regelgevingen die elk de verwerkte informatie en het doel van de verwerking vastleggen.
- DEUCC : het Samenwerkingsakkoord van 14 juli 2021
  o art. 11 bepaalt de informatie die verwerkt wordt in de certificaten die gebruikt worden om een CST te genereren
- CST : het Samenwerkingsakkoord van 14 juli 2021 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVIDcertificaat, het Covid Safe Ticket, het PLF en de verwerking van persoonsgegevens van in het buitenland wonende of verblijvende werknemers en zelfstandigen die activiteiten uitvoeren in België
  o art. 12 bepaalt de gegevens die verwerkt worden in het CST.
- Het samenwerkingsakkoord van 14 juli 2021 bepaalt de doelstelling van de verwerkingen.
- De noodzaak om CST als onderdeel van een toegangsbewijs te gebruiken wordt bepaald door het samenwerkingsakkoord van 14 juli 2021 en de overlegcomités die de maatregelen bepalen i.v.m. Corona.
- De memorie van toelichting van het samenwerkingsakkoord van 14 juli 2021 bepaalt ook de het strikt verboden is om het COVID Safe Ticket te genereren en in te lezen voor andere doeleinden dan deze gestipuleerd in dit samenwerkingsakkoord. Personen die het COVID Safe Ticket genereren of inlezen voor doeleinden die niet voorzien zijn in dit samenwerkingsakkoord, worden gestraft met gemeenrechtelijke sancties, inclusief strafrechtelijke sancties.	

Residueel risico	
De omschrijving is voldoende duidelijk en werd herhaald in het samenwerkingsakkoord tussen de verschillende overheden waardoor het risico hier beperkt is. De probabiliteit wordt actief gereduceerd door het wettelijke kader die de doelstellingen omschrijft.	
Risicoscore	
Probabiliteit na maatregelen	1

R04. Gespecificeerd doel	
Impact na maatregelen	2
Risico	LAAG

R05. Koppeling van doel aan gegevens

R05. Koppeling van doel aan gegevens
Kwetsbaarheid
Gegevens die alleen voor een bepaald doel opgeslagen en verwerkt worden, worden niet overeenkomstig gemarkeerd en/of beheerd.
Toelichting
Dit betreft een veiligheidsmaatregel waarbij voorkomen wordt dat de gegevens die zich op de verschillende systemen bevinden, zonder dat de beheerder van de informatie die intentie heeft, onterecht voor een andere verwerking worden gebruikt dan waarvoor de gegevens werden verzameld.
Maatregelen
Om de beslissingsmatrix die in het uitvoerend samenwerkingsakkoord van 27 september 2021 staat vermeld, uit te voeren, dient de CovidScan app een dynamische lijst met tijdelijk geschorste certificaten te downloaden vanaf een publieke website. Deze lijst dient door de CovidScan toepassing bewaard te worden op het mobiele toestel van de gebruiker die de CST zal aanmaken. Deze lijst wordt enkel voor dit doel gebruikt. Verder bepaalt het samenwerkingsakkoord dat de gegevens rond CST enkel mogen verwerkt en opgeslagen worden voor het genereren en controleren van CST.
Residueel risico
Door de methode van werken bestaat de kans dat de lijst met tijdelijk geschorste certificaten door andere toepassingen dan de CovidScan app wordt gedownload en bewaard. Toch zal de impact hiervan beperkt zijn omdat zonder bijkomende sleutel er geen link kan gemaakt worden tussen ID van het vaccinatiecertificaat en de betrokkene aan wie dit certificaat toebehoort.
Risicoscore

Probabiliteit na maatregelen	2
Impact na maatregelen	1
Risico	LAAG

R06. Gebruik gegevens buiten het doel

R06. Gebruik gegevens buiten het doel
Kwetsbaarheid
Verzamelde gegevens worden verwerkt voor andere doeleinden dan het doel waarvoor zij oorspronkelijk werden verkregen. Deze verschillende doeleinden zijn niet compatibel met het oorspronkelijke doel.
Toelichting
De geïdentificeerde risico's zijn de volgende: - Bijhouden van gescande certificaten in de app die het CST genereert en de link met de betrokkene - Opslaan van de lijsten van geschorste vaccinatiecertificaten Uit beide types van informatie kunnen er gezondheidsgegevens worden afgeleid van de betrokkene. Een herstelcertificaat zal aangeven of een betrokkene in een verleden korter dan 180 dagen geleden getroffen is geweest door een COVID infectie, een vaccinatiecertificaat geeft de vaccinatiestatus aan van een betrokken houder. De lijst van vaccinatiecertificaten die tijdelijk geschorst zijn zou kunnen toelaten na te gaan wie besmet werd geraakt.

R06. Gebruik gegevens buiten het doel
Het valt op te merken dat hoewel dit informatie betreft aangaande de gezondheid van een betrokkene, er geen bijkomende informatie zoals ziektebeeld, symptomatisch of asymptomatisch en behandeling kan afgeleid worden.
Maatregelen
Het gebruik van de CovidScan app is verplicht wanneer een CST gegenereerd wordt. Doordat deze toepassing beschikbaar gemaakt wordt door de overheid wordt een beperking voorzien van de informatie die verwerkt en bewaard wordt. De lijst van geschorste certificaten dient equivalent aan gepseudonimiseerd beschouwd te worden. Dit is noodzakelijk omdat de informatie dient verwerkt te worden door CovidScan app en omdat de bijkomende beschermingsmaatregelen tijdens transmissie van deze lijst en bewaring door de app alleen niet als voldoende kunnen worden beschouwd[6]. Om de informatie terug te leiden naar een betrokkene dient men over de informatie op het platform waar de informatie nodig voor het aanmaken van het DEUCC en de resultaten van testen bewaard worden te beschikken. Dit platform wordt terdege beschermd omdat deze de kritische informatie over de certificaten en de houders ervan bevat. Bijkomend geldt dat wanneer de informatie van dit platform zou lekken er geen bijkomend risico is dat de lijst van geschorste certificaten bijkomende informatie bovenop dit lek zou vrijgeven. In die zin creëert de publicatie van de lijst van geschorste certificaten geen bijkomend significant risico. De lijst en de informatie in de lijst worden op hun beurt beschermd waardoor checks buiten de CovidScan app om sterk bemoeilijkt worden.
Residueel risico
Het residueel risico is dat een bij de aanmaak van een CST zonder gebruik de COVIDScan app de gegevens van de houder van een certificaat kunnen gelinked worden aan de ID's van de geschorste certificaten. Dit zou kunnen gecombineerd worden met eerdere, huidige en toekomstige lijsten van geschorste certificaten waardoor een burger zou kunnen getracked worden op mogelijke besmettingen. Wanneer deze situatie zich zou voordoen, dan heeft deze enkel betrekking op de houders van een certificaat wiens DEUCC onrechtmatig werd gescand.

Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	2
Risico	LAAG

D03. Naleving van dataminimalisatie

Principe	Verzamel alleen persoonlijke informatie als u het echt nodig hebt
Samenvatting	Identificeer elk element van persoonlijke gegevens die u gebruikt en ga na of dit noodzakelijk is voor de verwerking. Wat is het doel van het verzamelen van de persoonlijke gegevens die hier zijn betrokken? Hoe kan de organisatie doen wat ze moet doen? Verzamelt u alleen wat u echt nodig hebt? Hebt u bijvoorbeeld echt "geboortedatum" nodig, of zal "leeftijd" of "ouder dan 18" voldoende zijn?
Link AVG	Artikel 5 c) gegevens toereikend, ter zake en beperkt

R07. Verzamelen van irrelevante gegevens

R07. Verzamelen van irrelevante gegevens
Kwetsbaarheid

[6] De maatregelen verwerkt in de app om de lijst te beschermen steunen op beveiliging van het platform waarop de app draait en de onmogelijkheid om met analytische middelen de beveiliging te verwijderen. Beide middelen worden als niet voldoende geëvalueerd. Om die reden wordt de beveiliging door de app enkel beschouwd als verhogen van de complexiteit om de lijst in te lezen. De bescherming door equivalentie aan pseudonimisatie blijft dan nog als beveiligingsmaatregel over.

R07. Verzamelen van irrelevante gegevens	
De betrokkene dient persoonlijke gegevens te verstrekken die niet relevant zijn voor het opgegeven doel van de verwerking of de bekomen gegevens zijn niet relevant voor het genereren van een CST.	
Toelichting	
De verzamelde gegevens dienen beperkt te zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking"). De verwerkte gegevens worden bepaald in de samenwerkingsakkoorden die afgesloten zijn betreffende het CST. Een uitzondering hierop is de lijst van certificaten die tijdelijk geschorst zijn. In de lijst van de certificaten die tijdelijk geschorst zijn zullen andere ID's van certificaten terug te vinden zijn dan degene die op een moment door de houder van een certificaat voorgelegd wordt aan de CovidScan app. Dit is echter noodzakelijk omdat de CovidScan app ook moet kunnen gebruikt worden wanneer deze geen internet toegang heeft. Hierdoor is het noodzakelijk dat de lijst volledig ter beschikking is.	
Maatregelen	
De burger dient zijn DEUCC voor te leggen opdat zijn CST zou gegenereerd kunnen worden. Deze certificaten kunnen meer informatie bevatten dan strikt noodzakelijk voor het genereren van het CST. Doordat het gebruik van de CovidScan app verplicht is bij het inlezen van DEUCC voor het genereren van CST en deze conform de samenwerkingsakkoorden de gegevensverwerking sterk beperkt, wordt tegengegaan dat er irrelevante gegevens worden verwerkt. De betrokkene wordt gevraagd enkel zijn DEUCC te tonen, eventueel ook een bewijs van identiteit dat kan gelinkt worden met het CST. Ook hiervoor voorziet CovidScan dat er geen informatie hierover verzameld wordt.	
Residueel risico	
Bij het gebruik van de CovidScan app worden geen verdere gegevens verwerkt.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R08. Minimaal gebruik van gegevens

R08. Minimaal gebruik van gegevens
Kwetsbaarheid
Er worden geen maatregelen genomen om ervoor te zorgen dat alleen relevante gegevens worden verwerkt en dat ze enkel worden verwerkt in relatie tot het doel.
Toelichting
De verzameling van verwerkte gegevens dient beperkt te zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking"). Dit betekent dat op het platform of de app, door verrijking of op een andere manier verworven gegevens, geen gegevens mogen verwerkt worden die niet noodzakelijk zijn voor de beoogde doelstellingen.
Maatregelen
De gegevens die verwerkt worden in het DEUCC en het CST zijn bepaald in de Europese verordening en de verschillende samenwerkingsakkoorden. De test-, herstel- en vaccinatie certificaten zijn op die regelgevingen afgestemd waardoor de verwerking enkel relevante gegevens bevat. Door het verplichten van de CovidScan app voor de genereren van het CST wordt ook de mogelijkheid beperkt om andere gegevens te verwerken in het CST en voorkomen secundaire verwerkingen te verrichten op de bekomen gegevens.
Residueel risico
Het residuele risico zal hier ontstaan wanneer er gebruik gemaakt wordt van een andere toepassing dan CovidScan. Op die manier zou dan meer informatie kunnen afgeleid worden uit de certificaten dan strikt noodzakelijk voor het genereren van het CST.

R08. Minimaal gebruik van gegevens	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	2
Risico	LAAG

D04. Waarborgen van de kwaliteit van persoonsgegevens

Principe	Zorg ervoor dat uw persoonlijke gegevens juist, relevant en up-to-date zijn voordat u deze gebruikt
Samenvatting	Er worden redelijke stappen ondernomen om de kwaliteit te waarborgen, afhankelijk van de betreffende informatie. Relevante factoren zijn onder meer: welk proces is er om te controleren of de informatie juist is? Is de informatie rechtstreeks door de persoon verstrekt? Is het rechtstreeks met de persoon gecontroleerd? Is het geautomatiseerd, of kunt u menselijk oordeel toepassen? Hoe schadelijk is het voor het individu als informatie verkeerd of misleidend is? (Hoe schadelijker het wordt, hoe uitgebreider de stappen moeten zijn voor het controleren van de nauwkeurigheid)
Link AVG	Artikel 5 d) gegevens juist zijn en zo nodig worden geactualiseerd

R09. Volledigheid en juistheid van gegevens

R09. Volledigheid en juistheid van gegevens
Kwetsbaarheid
Bij het verzamelen en verkrijgen van gegevens wordt er niet voldoende gecontroleerd op volledigheid en juistheid van de gegevens
Toelichting
Er is een risico dat - een gebruiker een DEUCC voorlegt dat niet aan de gebruiker toebehoort waardoor verkeerdelijk toegang wordt verleend - de lijst van tijdelijk geschorste vaccinatiecertificaten niet correct is waardoor ten onrechte toegang wordt verleend of geweigerd - de lijst van tijdelijk geschorste vaccinatiecertificaten niet recent genoeg is waardoor ten onrechte toegang wordt verleend of geweigerd. Het risico dat een certificaat ten onrechte wordt toegekend of foutieve informatie bevat wordt niet opgenomen in deze lijst. Dit risico dient deel uit te maken van een andere GEB.
Maatregelen
- in een DEUCC en CST worden de naam en de voornaam van de houder van het certificaat vermeld. Op basis van een identiteitscontrole kan dan eenvoudig nagegaan worden of de houder van het certificaat ook degene is die het vertoont. - De lijst van certificaten die tijdelijk geschorst zijn wordt getekend door de uitgever middels asymmetrische sleutels. Met gebruik van de publieke sleutel kan nagegaan worden of de lijst effectief door de juiste entiteit werd uitgegeven. Dit zit verwerkt in de CovidScan app. - Wanneer de CovidScan app gedurende 24 uur geen updates van de lijst van tijdelijk geschorste certificaten kan bekomen zal de CST module niet langer werken.
Residueel risico
De risico's zoals hierboven aangehaald werden op adequate wijze weggewerkt. Het residuele risico bestaat erin dat de private sleutel waarmee de lijst van geschorste certificaten getekend wordt, gelekt is en er corrupte lijsten worden doorgestuurd.
Risicoscore

R09. Volledigheid en juistheid van gegevens	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R10. Accuraatheid en actueelheid van gegevens

R10. Accuraatheid en actueelheid van gegevens
Kwetsbaarheid
Er zijn geen procedures geïmplementeerd die regelmatig controleren of de persoonsgegevens accuraat en actueel zijn.
Toelichting
CST heeft als doelstelling een onderdeel te zijn van een beslissingsproces om toegang te verlenen tot een evenement of een horecazaak of sportclub. Wanneer de informatie niet accuraat is dan ontstaat de mogelijkheid dat de betrokkene onterecht toegang wordt geweigerd of toegekend. Voor elk certificaat dient de informatie uit de QR code van het DEUCC gelezen te worden en nadien bijkomend de lijst met IDs van certificaten die geschorst zijn te worden geconsulteerd. Het risico R10 kan dus ontstaan wanneer deze lijst niet correct of actueel is.
Maatregelen

• De lijst van certificaten die geschorst zijn wordt getekend door de uitgever middels asymmetrische sleutels. Met gebruik van de publieke sleutel kan nagegaan worden of de lijst effectief door de juiste entiteit werd uitgegeven. Dit zit verwerkt in de CovidScan app.
• Wanneer de CovidScan app gedurende 24 uur geen updates van de lijst van tijdelijk geschorste certificaten kan bekomen zal deze module niet langer werken.
• De lijst van certificaten die geschorst zijn wordt op regelmatige basis opgesteld vanaf de authentieke bronnen (resultaten van PCR testen afgeleverd door Sciensano en certificaten beheerd door de bevoegde instelling) en verder aangevuld met
  ○ Naast publicatie certificaatcodes t.g.v. positieve test
  ○ Toevoegen van de geschorste certificaatcodes
  ○ Toevoegen van dummy certificaatcodes
• De Gemengde samenstelling van de lijst van certificaatcodes wordt opgemaakt zonder het vermelden van de reden van opname op de lijst

Residueel risico
Doordat het risico reeds vervat zit in R.09 blijft het risico op hetzelfde niveau als bij R.09
Risicoscore

Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R11. Verrijking van gegevens

R11. Verrijking van gegevens
Kwetsbaarheid
Persoonlijk identificeerbare profielen van betrokkenen worden door probabilistische algoritmen verrijkt met onjuiste informatie
Toelichting
De uitwisseling van gegevens betreft: • Gegevens in de QR code van de DEUCC voorgelegd door de houder van het certificaat • Gegevens die nodig zijn voor de verwerking van CST

R11. Verrijking van gegevens
De QR code bevat meer gegevens dan strikt noodzakelijk voor het aanmaken van het CST. Het verplichte gebruik van CovidScan app zal ervoor zorgen dat er verwerking gebeurt van enkel de informatie nodig om dit CST aan te maken. Het risico dient dus gevonden te worden buiten het gebruik van de daartoe voorziene app en van informatie die al dan niet publiek beschikbaar is.
Maatregelen
Het verplichte gebruik van de app voor het controleren van de voorwaarden om al dan niet toegang te verlenen tot bv. een horecazaak voorkomt dat er informatie die niet noodzakelijk is verwerkt wordt. De lijst met ID's van certificaten die geschorst zijn zou kunnen verrijkt worden met gegevens bekomen van de betrokkenen. Echter, wanneer de lezing van de QR code gebeurt met de CovidScan app dan zal ook deze informatie niet verder verwerkt en bewaard worden.
Residueel risico
Bij het tonen van zijn certificaat zal bij de controle mogelijk de ID leesbaar zijn, hetzij bij de QR code, hetzij op het papieren document en kan daarvan een foto genomen worden. Omdat de naam van de persoon erbij staat, samen met enkele andere gegevens laat dit toe de houder van DEUCC te identificeren. Op die manier kan door oneigenlijk inlezen het ID van het certificaat gekoppeld worden aan de gebruiker ervan. Op die manier kan een lijst aangelegd worden van personen met een vaccinatiecertificaat en van personen die een herstelcertificaat hebben. Omdat de lijst met IDs van certificaten die geschorst zijn rechtstreeks afgeleid wordt van een positieve PCR test kan daardoor voor het verleden en de toekomst een deel van de gezondheidsstatus van de betrokkene gevolgd worden. De impact daarvan is eerder beperkt gezien de lijst geen reden bevat waarom een certificaat op de lijst voorkomt. De partij die deze methode toepast stelt zich door deze actie bloot aan gerechtelijke en strafrechtelijke vervolging.
Risicoscore

Probabiliteit na maatregelen	1
Impact na maatregelen	2
Risico	LAAG

D05. Naleving van de vereisten inzake opslagbeperking

Principe	Verwijder de data van zodra u deze niet meer nodig hebt
Samenvatting	Hoe lang bent u van plan de informatie te bewaren? Zijn er verplichtingen om de informatie voor een bepaalde periode te houden, zoals onder regelgeving of wetgeving? Als er geen dergelijke verplichtingen bestaan, wat zou dan als een redelijke periode worden beschouwd om de informatie te bewaren? Hoe zit het met beroepsprocedures en verjaringstermijnen? Hoe gaat u hiermee over weg? Wanneer informatie met een derde partij wordt gedeeld, overweeg dan hoe lang zij de informatie zullen bewaren en welke stappen er zijn om ervoor te zorgen dat zij beschikken over persoonlijke informatie wanneer de bedrijfsvereisten zijn voltooid.
Link AVG	Artikel 5 e)

R12. Verwijderen van gegevens

R12. Verwijderen van gegevens
Kwetsbaarheid
Persoonsgegevens en bijbehorende back-upgegevens worden niet verwijderd of geanonimiseerd wanneer opslag niet meer nodig is voor het opgegeven doel.
Toelichting

R12. Verwijderen van gegevens	
Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is, dienen de bewaartermijnen vastgesteld te stellen voor het wissen van gegevens of voor een periodieke toetsing ervan. Bij ontbreken van een behoorlijk beleid hieromtrent wordt het principe van dataminimisatie met de voeten getreden. In het samenwerkingsakkoord van 14 juli 2021 geeft artikel 14§2 aan dat de gegevens verwerkt voor het genereren van CST onmiddellijk worden verwijderd na de verwerking.	
Maatregelen	
De maatregelen zitten ingebakken in de CovidScan app.De app is ontwikkeld door Digitaal Vlaanderen op instructie van eHealth Platform en volgt deze regel. De lijst van ID's van certificaten die tijdelijk geschorst zijn wordt eveneens op de app gedownloaded. Omdat er per uur een nieuwe update is, wordt deze lijst na verloop van tijd verwijderd. Dit betekent niet dat de lijst na een uur wordt verwijderd op het toestel. De app blijft immers werken op een lijst die maximaal 24 uur oud is. Wanneer de lijst ouder zou zijn, dan kunnen geen vaccinatiecertificaten door de app verwerkt worden.	
Residueel risico	
De CovidScan app werkt op het OS van een mobiel toestel dat onder controle is van de gebruiker. Indien het toestel corrupt is, dan kan het verwijderen van informatie verhinderd worden. Dit is van toepassing op informatie verzameld bij het inlezen van een certificaat als voor het verwijderen van de lijst van ID's van certificaten die geschorst zijn. De kans bestaat dat de gebruiker door middel van analytische methodes de software kan aanpassen zodat de gegevens niet langer op correcte wijze verwijderd worden en de lijst met ID's van geschorste certificaten bewaard blijft. Toch is de kans dat de gegevens uit deze lijst bruikbaar zijn beperkt door de beschermende maatregelen die van toepassing zijn op de suspension list.	
Risicoscore	
Probabiliteit na maatregelen	2
Impact na maatregelen	2
Risico	MEDIUM

R13. Gebruiken van niet-verwijderde gegevens

R13. Gebruiken van niet-verwijderde gegevens
Kwetsbaarheid
Persoonsgegevens, die niet langer nodig zijn voor het opgegeven doel, maar niet kunnen worden verwijderd omwille van retentieregels, kunnen niet worden uitgesloten van de reguliere gegevensverwerking.
Toelichting
Er zijn geen technische maatregelen die voorzien dat gegevens langer bewaard worden dan nodig of die niet toelaten dat data uit de app worden verwijderd.
Maatregelen
Wanneer de lijst van ID's van certificaten die geschorst zijn niet tijdig wordt vervangen dan voorziet de app dat 24 uur nadat de laatste lijst werd gedownload, er geen CST meer kunnen uitgereikt worden. Wanneer de lijsten bijgehouden worden zou deze kunne gebruikt worden om de infectiegeschiedenis van een toonder van de certificaat te achterhalen. Deze mogelijkheden worden beperkt door de beschermingsmaatregelen die van toepassing zijn op de suspension list.
Residueel risico
De CovidScan app werkt op het OS van een mobiel toestel dat onder controle is van de gebruiker. Indien het toestel corrupt is, dan kan het verwijderen van informatie verhinderd worden. Dit is van toepassing op informatie verzameld bij het inlezen van een certificaat als voor het verwijderen van de lijst van ID's van certificaten die geschorst zijn.

R13. Gebruiken van niet-verwijderde gegevens	
De kans bestaat dat de gebruiker door middel van analytische methodes de software kan aanpassen zodat de gegevens niet langer op correcte wijze verwijderd worden. Door middel van analytische methodes zou de gebruikte versleuteling kunnen ongedaan worden of gebruikt worden in andere toepassingen om gegevens zoals de lijst van IDs van certificaten die geschorst zijn te downloaden. De kans dat dit gebeurt wordt echter beperkt door de veiligheidsmaatregelen van toepassing op de suspension list.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	2
Risico	LAAG

D06. Naleving van het recht op bescherming van vertrouwelijkheid en veiligheid van de gegevensverwerking

Principe	Behandel de data waarover u beschikt als een 'goede huisvader' en bescherm het tegen verlies, ongeoorloofde toegang en gebruik, wijziging of openbaarmaking en ander misbruik.
Samenvatting	Er kunnen een aantal methoden zijn om u te helpen de persoonlijke informatie die u bezit te beschermen, zoals beleid en gedragscodes die bepalen hoe werknemers persoonlijke informatie behandelen, tot fysieke of technische controles die de informatie beschermen. Het is handig om rechtstreeks naar documenten of informatie te verwijzen die beschikbaar zijn om dit te ondersteunen. Waarborgen kunnen zijn: fysieke beveiliging; IT beveiliging; opleiding van het personeel; beleid dat medewerkers moeten naleven; vertrouwelijkheidsclausules in contracten met externe providers, enz. Overweeg of er kwetsbaarheden zijn in elk deel van het informatie verwerkingsketen - identificeer zwakke verbindingen
Link AVG	Artikel 5 f) een passende beveiliging van de gegevens is gewaarborgd

R14. Ongeautoriseerde toegang tot gegevens

R14. Ongeautoriseerde toegang tot gegevens
Kwetsbaarheid
De gegevens worden onvoldoende beveiligd, waardoor persoonsgegevens kunnen worden gestolen, of geraadpleegd door iemand die daartoe niet gerechtigd of gemachtigd is
Toelichting
Bij het genereren van CST wordt informatie uit volgende bronnen verwerkt: - DEUCC aangeboden door de houder van het certificaat - Lijst van ID's van certificaten die geschorst zijn De app CovidScan is het enige middel dat toegelaten is om CST aan te maken.
Maatregelen
- de wetgever heeft voorzien dat CST enkel met behulp van CovidScan mag gegenereerd worden. Dit betekent dat de verwerking gebeurt conform de bepalingen vastgelegd in de relevante wetten en voorziet geen bewaring van de gegevens. - De wetgever heeft ook het kader omschreven dat bepaalt wie de gegevens op de DEUCC mag verwerken voor het genereren van CST.
Residueel risico
De residuele risico kunnen als volgt opgelijnd worden:

R14. Ongeautoriseerde toegang tot gegevens	
- Lek van gegevens uit de toepassing CovidScan naar het OS of een andere toepassing van een gehackte telefoon - Lek van gegevens uit de lijst van ID's van certificaten die geschorst zijn door omzeiling van de veiligheidsmaatregelen die op de gegevens in de telefoon zijn toegepast. Vanwege het gepseudonimiseerde karakter van de gegevens is de impact hiervan zeer beperkt. - Omzeilen van de verplichting van het gebruik van de CovidScan app waardoor andere gegevens op het certificaat verwerkt worden. De gegevens waartoe toegang kan genomen worden betekenen echter een beperkt risico voor de betrokkene. Over het algemeen kan gesteld worden dat onrechtmatig toegang tot deze informatie geen hoge impact zal hebben voor de betrokkene. Er wordt immers geen reden gegeven waarom een certificaat geschorst werd. Voor de informatie over de vaccinatie heeft de wetgever voorzien dat de vaststelling of iemand al dan niet gevaccineerd is niet mag leiden tot een aparte behandeling. Indien vaccinatie een voorwaarde is voor medewerkers van bedrijven dan kan deze informatie over medewerkers enkel bekomen worden wanneer daar een wettelijke basis voor gecreëerd werd. Wanneer een aanval zou gebeuren na harvesting van certificate ID's van vaccinatiecertificaten die tijdelijk geschorst zijn (bv. door phishing) dan kan de aanvaller deze ID's van vaccinatiecertificaten die tijdelijk geschorst zijn mogelijks checken in de suspension list. Toch blijft de kans dat dit gebeurt beperkt door de beschermingsmaatregelen van de lijst en de obfuscatie van de software wat reverse engineering moeilijk maakt.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	2
Risico	LAAG

R15. Pseudonimisatie van gegevens

R15. Pseudonimisatie van gegevens
Kwetsbaarheid
De gegevens zijn niet geanonimiseerd of gepseudonimiseerd, waardoor de persoonsgegevens direct kunnen worden gelinkt met de betrokkene
Toelichting
De CovidScan app is gericht om een DEUCC in te lezen, het resultaat zichtbaar te maken aan degene die instaat voor toegangscontrole. Deze laatste moet ook de mogelijkheid hebben om na te gaan of het gepresenteerde DEUCC representatief is voor de persoon die het presenteert. Om die reden kan de informatie niet gepseudonimiseerd worden tijdens de verwerking.
Maatregelen
Omdat de gegevens niet gepseudonimiseerd kunnen verwerkt worden, dient voorzien te worden dat deze informatie niet verder kan verwerkt worden. Om die reden werd de CovidScan ontwikkeld. De lijst van ID's van certificaten die geschorst zijn bevat enkel de ID's. Deze ID's zijn totaal willekeurig gekozen en laten niet toe om de identiteit van de houder van het certificaat te identificeren zonder dat er bijkomende informatie beschikbaar is.
Residueel risico
Bij normaal gebruik van CovidScan voor het genereren van de CST is het residueel risico onder controle. De garanties van de aan pseudonimisatie equivalente bescherming van de lijst van ID's van certificaten die geschorst zijn hangt af van de bescherming van de informatie die deze ID's kan linken aan de houder van het certificaat. Wanneer deze informatie zou lekken, dan is de impact nog steeds beperkt. Er wordt immers geen reden gegeven waarom een certificaat geschorst werd.
Risicoscore

Probabiliteit na maatregelen	1

R15. Pseudonimisatie van gegevens	
Impact na maatregelen	2
Risico	MEDIUM

R16. Verlies van gegevens

R16. Verlies van gegevens
Kwetsbaarheid
Er worden geen maatregelen genomen om ervoor te zorgen dat de verdwijning (onopzettelijk verlies, vernietiging of beschadiging) of onbeschikbaar zijn van persoonsgegevens kunnen worden teniet gedaan.
Toelichting
Het risico dat hier beschouwd wordt is dat een CST niet kan gegenereerd worden op basis van een DEUCC. De onbeschikbaarheid van een DEUCC voor een burger wordt in deze GEB niet opgenomen. Het genereren van een CST gebeurt door de app CovidScan o.b.v de DEUCC en de suspension list. Wanneer deze externe lijst niet beschikbaar is gedurende een periode van 24 uur, dan zal er geen CST meer kunnen gegenereerd worden en kan geen toegang meer verleend worden tot een evenement of een horecazaak.
Maatregelen
Indien de app CovidSanBe gedurende meer dan 24 uur niet online was, zal de app onbruikbaar worden tot op het moment dat deze opnieuw online komt, tot dan kunnen geen nieuwe CST's gevalideerd worden
Residueel risico
Ondanks de beste voorzieningen kan het nog steeds voorkomen dat de terbeschikkingstelling van de lijst met ID's van de certificaten die geschorst zijn onderbroken is. Op dat moment zal de CovidScan app na 24 uur geen CST kunnen uitreiken aan houders van een vaccinatiecertificaat.
Risicoscore

Probabiliteit na maatregelen	1
Impact na maatregelen	3
Risico	MEDIUM

R17. Detectie van datalekken

R17. Detectie van datalekken
Kwetsbaarheid
Er is geen mechanisme dat automatisch datalekken detecteert waardoor datalekken blijven aanhouden
Toelichting
De gegevens die worden gebruikt zijn beschikbaar op het getoonde DEUCC of in de lijst van ID's van vaccinatiecertificaten die tijdelijk geschorst zijn. Het beheer en bescherming van DEUCC is geen onderwerp van deze GEB. Om die reden worden de risico's gerelateerd tot de bescherming ervan niet verder gedetailleerd. De manier waarop de lijst van ID's van certificaten die geschorst zijn opgesteld wordt en de informatie die deze bevat maakt dat deze een bescherming equivalent aan pseudonimisering van persoonsgegevens heeft waardoor bij een eventueel lek geen bijkomende risico's optreden. De lijst zelf is publiek met extra beveiligingsmaatregelen tegen gebruik buiten de app.
Maatregelen
De suspension list wordt extra beschermd tegen gebruik buiten de app.
Residueel risico
Wanneer een aanvaller dmv phising aan harvesting doet van Certificate ID's van vaccinatiecertificaten die tijdelijk geschorst zijn, dan zou deze de gezondheidstoestand van de betrokkene kunnen volgen. Toch is dit risico beperkt door bescherming van de suspension list en

R17. Detectie van datalekken	
de bijkomende mogelijkheid om certificaten tijdelijk te schorsen zonder impact op de betrokkene en de bevolking.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R18. Testen van beveiligingsmaatregelen

R18. Testen van beveiligingsmaatregelen	
Kwetsbaarheid	
De geïmplementeerde beveiligingsmaatregelen worden niet op gezette tijdstippen getest, beoordeeld of geëvalueerd?	
Toelichting	
Beveiligingsmaatregelen zijn noodzakelijk voor de bescherming van de persoonsgegevens die op het platform en op de smartphones van de gebruikers aanwezig zijn. Wanneer relevant, dienen deze maatregelen op regelmatige tijdstippen getest te worden om hun efficiëntie te meten. In het geval van CST wordt de informatie bekomen vanaf het DEUCC dat voorgelegd wordt en de lijst met ID's van certificaten die geschorst zijn. Bij deze laatste zijn vooral de integriteit en beschikbaarheid van groot belang.[7] De betrokkene kan zijn DEUCC bekomen met gebruik van ITSME (CovidSafe app) of FAS authorisatie niveau 350 wanneer dit certificaat gedownload wordt vanaf het internet. Deze middelen zijn door de federale overheid als "Substantial" of "Hoog" gekwalificeerd. Vanaf dat moment zal de gebruiker zelf verantwoordelijk zijn voor de bescherming van de informatie op de systemen waar de gebruiker gebruik maakt. De beveiliging van het platform waarop de DEUCC beschikbaar zijn zelf is geen onderdeel van deze GEB.	
Maatregelen	
De sleutel om de integriteit van de lijst met ID's van certificaten die geschorst zijn te controleren zit ingebed in de app. Wanneer de lijst met ID's van certificaten die geschorst zijn zou aangepast zijn, dan wordt dit automatisch gemerkt door de CovidScan app. Dit geldt ook voor andere veiligheidsmaatregelen die toegepast zijn om de lijst met ID's van certificaten die tijdelijk geschorst zijn te beschermen.	
Residueel risico	
De checks die in de CovidScan app worden gebruikt zijn afdoende om de risico van het proces op deze kwetsbaarheid tot voldoende laag niveau te beperken.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R19. Procedure Datalekken

R19. Procedure Datalekken
Kwetsbaarheid
Er is geen procedure om betrokkenen op de hoogte te brengen in het geval van een datalek
Toelichting

[7] De confidentialiteit m.b.t. de houders van de certificaten wordt inhoudelijk beschermd en werd besproken in vorige delen van de analyse waardoor deze hier niet verder dient besproken te worden.

R19. Procedure Datalekken
Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee. De in bedoelde mededeling aan de betrokkene is niet vereist wanneer: • passende technische en organisatorische beschermingsmaatregelen genomen zijn • de mededeling onevenredige inspanningen zou vergen Het genereren van een CST op basis van een DEUCC dient te gebeuren op een mobiel toestel en gebruikt hiervoor de CovidScan app. De verzamelde informatie is sterk beperkt en mag niet opgeslagen worden. Het aanreiken van de DEUCC wordt behandeld in een andere GEB. De lijst met ID's van certificaten die geschorst zijn wordt op hetzelfde platform aangemaakt. De informatie vervat in de lijst met ID's van certificaten die geschorst zijn wordt beschermd door een equivalente bescherming als pseudonimisatie waarbij het belangrijk is de link tussen het ID van het geschorste certificaat en de betrokken houder ervan niet vrij te geven. Indien dit zou gelekt worden, dan zal hierdoor informatie die de gezondheid betreft gelekt worden. Het lek betreft dan de informatie in de lijst met ID's van certificaten die geschorst zijn. Deze lijst is een uittreksel van de informatie in de database waar een lek zou zijn. Het is daarom niet noodzakelijk om specifiek voor het lek van de lijst met ID's van certificaten die geschorst zijn een aparte communicatie te voorzien gezien deze reeds in de communicatie over het lek van de database moet afgedekt zijn.
Maatregelen
Geen bijzondere bijkomende maatregelen.
Residueel risico
Er is geen bijkomend residueel risico ten opzichte van het risico dat ontstaat wanneer er zich een lek zou voordoen met de gegevens van de database beheerd door Vlaanderen Digitaal en die de informatie over de DEUCC bevat.

Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R42. Blootstelling van gegevens aan derden

R42. Blootstelling van gegevens aan derden
Kwetsbaarheid
Gegevens die niet vallen onder het genereren van het CST worden blootgesteld aan derden als gevolg van de ingebruikname van de applicatie.
Toelichting
CST wordt afgeleid van het DEUCC. De gebruiker zal deze moeten voorleggen aan de wachter die deze zal scannen. Hiertoe is de DEUCC voorzien van een QR code. De QR code bevat gegevens die niet strikt noodzakelijk zijn voor het creëren van een CST. Toch zullen deze gegevens leesbaar zijn en zouden deze kunnen gebruikt worden voor verdere (onrechtmatige) verwerking.
Maatregelen
De wetgever heeft in het samenwerkingsakkoord van 14 juli 2021voorzien dat: - voor het genereren van het CST enkel mag gebruik gemaakt worden van de CovidScan app. Deze app zal het principe van dataminimisatie toepassen en niet onnodig gegevens verwerken Ook voorziet de app dat gegevens niet bewaard worden op het toestel. - De inhoud van CST zodanig bepaald is, dat enkel de noodzakelijke informatie, nodig voor het vaststellen of toegang kan verleend worden verwerkt wordt. Met deze maatregel wordt het aantal blootgestelde gegevens sterk beperkt

R42. Blootstelling van gegevens aan derden	
De suspension list bevat informatie die van nature beschermd wordt door een aan pseudonimisatie equivalente bescherming en bijkomende beveiliging. Hierdoor wordt de kans op lekken of informatie terugbrengen tot een betrokkene sterk beperkt	
Residueel risico	
Er blijft een residueel risico dat bij voorleggen van DEUCC geen gebruik gemaakt wordt van de CovidScan app. Wanneer de QR code wordt ingelezen of wanneer bijkomende informatie van het certificaat wordt gefotografeerd, dan wordt informatie die niet noodzakelijk is voor het genereren van de CST beschikbaar gesteld aan derden. Dit risico is en blijft inherent aan het gebruik van DEUCC waarvoor het formaat en inhoud bepaald wordt door de Europese instellingen. Toch moet de impact hiervan als middelmatig moet beschouwd worden. De informatie op een ticket geeft een feitelijke toestand weer. Voor wat betreft de kennis rond type van vaccinatie heeft de wetgever op dit moment niet voorzien dat er enig verschil is in de bewegingsvrijheid die een gevaccineerd persoon krijgt in functie van het type vaccin dat werd toegediend.	
Risicoscore	
Probabiliteit na maatregelen	2
Impact na maatregelen	2
Risico	MEDIUM

D07. Rechtmatigheid van de verwerking van persoonsgegevens

Principe	Is er voldaan aan één van de voorwaarden waardoor de verwerking rechtmatig mag genoemd worden?
Samenvatting	Het verwerken van persoonsgegevens is niet gebaseerd op: contractuele relatie, wettelijke verplichting, algemeen belang, gerechtvaardigde belangen, toestemming, vitaal belang Er is legitimiteit voor de verwerking van: bijzondere categorieën van persoonsgegevens persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten
Link AVG	Artikel 6 Rechtmatigheid van de verwerking Artikel 7 Voorwaarden voor toestemming Artikel 8 Voorwaarden voor de toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij Artikel 9 Verwerking van bijzondere categorieën van persoonsgegevens Artikel 10 Verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten

R20. Rechtmatigheid van verwerking

R20. Rechtmatigheid van verwerking
Kwetsbaarheid

R20. Rechtmatigheid van verwerking	
Het verwerken van persoonsgegevens is niet gebaseerd op: - contractuele relatie, - wettelijke verplichting, - algemeen belang, - gerechtvaardigde belangen, - toestemming, - vitaal belang	
Toelichting	
Opdat de gegevens kunnen verwerkt worden, dient een wettelijke basis voorzien te worden om de gegevens te verzamelen en verder te verwerken. De gegevens die worden verwerkt zijn medische gegevens waardoor er dient voldaan te worden aan de vereisten vermeld in artikel 6 en artikel 9 van de GDPR.	
Maatregelen	
De rechtmatigheid van de verwerking wordt onttrokken aan artikel 6.1 e van de AVG. Voor de verwerking van medische gegevens wordt een uitzondering op het principiële verbod bekomen door toepassing van artikel 9.2.i van de GDPR. Er is een wettelijk kader gecreëerd voor de toepassing van CST in de samenwerkingsakkoorden van 14 juli 2021 Deze voorzien de verwerkingen die mogen plaatsvinden om CST te genereren, het toepassingsgebied van de CST en de manier waarop dit CST mag aangewend worden. De wetgever legt ook vast dat het gebruik van CST voor gevallen die niet toegestaan zijn, verboden is.	
Residueel risico	
De regelgeving voorziet een beperkt aantal verwerkingen en duurtijd. Wanneer het toepassingsgebied uitgebreid zou worden of de duurtijd voor het gebruik van CST zal de wetgever hiervoor bijkomend een kader dienen te creëren en eventueel advies te vragen aan de Raad van State en de Gegevensbeschermingsautoriteit..	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R21. Toestemming voor verwerking

R21. Toestemming voor verwerking	
Kwetsbaarheid	
Indien gebaseerd op toestemming: Expliciete toestemming is niet verkregen of is verkregen op basis van onvolledige of onjuiste informatie of is verkregen op basis van een aanbod van voordeel of dreiging met nadeel.	
Toelichting	
Het gebruik van CST is opgelegd door de wetgever die hiervoor een wettelijke basis heeft vastgelegd. Bijgevolg is dit risico niet van toepassing	
Maatregelen	
N/A	
Residueel risico	
N/A	
Risicoscore	
Probabiliteit na maatregelen	NVT
Impact na maatregelen	NVT
Risico	NVT

R22. Legitimiteit verwerking bijzondere categorieën persoonsgegevens

R22. Legitimiteit verwerking bijzondere categorieën persoonsgegevens	
Kwetsbaarheid	
Er is geen legitimiteit voor het verwerken van bijzondere categorieën van persoonsgegevens	
Toelichting	
De AVG bepaalt dat gegevens zoals vermeld in artikel 9 en 10 niet mogen verwerkt worden. Voor deze toepassing betreft het gegevens zoals bepaald in artikel 9 §1. De AVG voorziet in uitzonderingen bepaald in artikel 9 §2 waardoor gegevens wel mogen verwerkt worden. Het algemeen belang van de toepassing van CST ligt in het beschermen van de volksgezondheid wat geldt als een voldoende reden vermeld in 9 §2.i waardoor het verbod niet van toepassing is.	
Maatregelen	
Er wordt dataminimisatie toepast bij het genereren van CST en het gebruik van DEUCC. Hierdoor wordt het aantal verwerkte gegevens sterk teruggedrongen en is de impact voor de betrokkenen sterk beperkt.	
Residueel risico	
Geen verder risico vastgesteld.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R23. Legitimiteit verwerken juridische persoonsgegevens

R23. Legitimiteit verwerken juridische persoonsgegevens	
Kwetsbaarheid	
Er is geen legitimiteit voor het verwerken van persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten	
Toelichting	
CST voorziet niet in de verwerking van deze gegevens.	
Maatregelen	
Niet van toepassing	
Residueel risico	
Niet van toepassing (NVT)	
Risicoscore	
Probabiliteit na maatregelen	NVT
Impact na maatregelen	NVT
Risico	NVT

R24. Verwerking gegevens van minderjarigen

R24. Verwerking gegevens van minderjarigen
Kwetsbaarheid
Kinderen zijn zich allicht minder bewust zijn van de betrokken risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van persoonsgegevens. Bij gebrek aan specifieke maatregelen kunnen zij aldus blootgesteld worden aan onbekende risico's
Toelichting
De toepassing van CST en DEUCC betreft alle personen vanaf de leeftijd van 12 jaar. Er dient daarom rekening gehouden te worden met het feit dat gegevens van minderjarigen verwerkt worden.

R24. Verwerking gegevens van minderjarigen	
Maatregelen	
Er zijn geen specifieke maatregelen genomen om de belangen van de minderjarigen in deze bijkomend te beschermen. De verplichting van het gebruik van CovidScan app voorziet in dataminimisatie en de wettelijke context die het toepassingsgebied bepaalt waar CST ingezet wordt beperkt het risico voor de betrokkenen van wie de gegevens verwerkt worden, inclusief de minderjarigen. Door het verplichte gebruik van CovidScan worden de maatregelen voorzien op een terdege bescherming van de verwerkte gegevens, inclusief die van de minderjarigen.	
Residueel risico	
Geen bijzonder risico voor de minderjarigen.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R43. Gebruik onder dwang

R43. Gebruik applicatie onder dwang	
Kwetsbaarheid	
De betrokkene wordt door een derde gedwongen de applicatie te installeren; of indien de levering van goederen en/of diensten en/of uitvoering van een overeenkomst voorwaardelijk wordt gesteld aan het installeren van de applicatie.	
Toelichting	
Derden zoals universiteiten, werkgevers, scholen, openbaar vervoer, overheidsinstanties, horeca, etc. zouden kunnen toegangsrestricties invoeren voor mensen die geen CST kunnen voorleggen	
Maatregelen	
Het samenwerkingsakkoord van 14 juli 2021 bepaalt dat burgers niet kunnen verplicht worden om de CovidSafe of de CovidScan app te installeren maar dat zij wel dienen te voldoen aan de gestelde voorwaarden om aan een evenement deel te nemen of toegang te verkrijgen tot een zaak. CST is gebaseerd op het gebruik van DEUCC en bevat 3 mogelijkheden om te voldoen aan de voorwaarden om een DEUCC en dus ook een CST te verkrijgen. In die zin leidt CST dus niet tot de verplichting zich te laten vaccineren. Als alternatief voorziet de uitgever van een certificaat in de mogelijkheid een DEUCC te downloaden of te bekomen op eenvoudige aanvraag. De wetgever voorziet de verplichting om een CST te genereren om toegang te verkrijgen tot bepaalde evenementen en zaken. Deze lijst is limitatief en dynamisch. Omwille van eerder vermeldde veiligheidsmaatregelen is de organisator van een evenement of uitbater van een zaak waar CST controle verplicht is, gedwongen de CovidScan app te gebruiken en dus ook te installeren.	
Residueel risico	
De wetgever voorziet de verplichting om een CST te genereren om toegang te verkrijgen tot bepaalde evenementen en zaken. De burger zal op dat moment verplicht zijn om aan de nodige voorwaarden te voldoen. Het valt op te merken dat het CST niet aan de basis van deze verplichting ligt maar wel het middel is om aan te tonen dat aan de voorwaarden wordt voldaan om aan een evenement deel te nemen of toegang te verkrijgen tot een zaak.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1

R43. Gebruik applicatie onder dwang	
Risico	LAAG

D08. Naleving van het recht op informatie (over gegevensverwerking)

Principe	Mensen kunnen hun persoonlijke gegevens zien als ze dat willen
Samenvatting	In dit gedeelte moet worden beschreven welke stappen de organisatie neemt om een persoon toegang te geven tot zijn informatie en hoe de organisatie omgaat met verzoeken om toegang. Kan het systeem zo worden ontworpen dat het eenvoudig is om mensen hun informatie te geven?
Link AVG	Afdeling 1 Transparantie en regelingen Artikel 12 Transparante informatie, communicatie Afdeling 2 Informatie en toegang tot persoonsgegevens Artikel 13 Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld Artikel 14 Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen Artikel 15 Recht van inzage van de betrokkene

R25. Toelichten impact gegevensverwerking

R25. Toelichten impact gegevensverwerking
Kwetsbaarheid
De impact van de gegevensverwerking is niet voldoende toegelicht aan de betrokkene.
Toelichting
De verwerkingsverantwoordelijke neemt passende maatregelen opdat de betrokkene de in de artikelen 13 en 14 bedoelde informatie en de in de artikelen 15 tot en met 22 en artikel 34 van de AVG bedoelde communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt, in het bijzonder wanneer de informatie specifiek voor een kind bestemd is. De informatie wordt schriftelijk of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen, verstrekt. Voor CST is de impact van de verwerking voor de betrokkene duidelijk. Wanneer er geen CST kan gegenereerd worden dan zal de betrokkene geen toegang verschaft worden. Er zijn geen andere verwerkingen voorzien. Het aanmaken van DEUCC is een verwerking die de creatie van het CST voorafgaat en is geen onderwerp van deze GEB vermits dit reeds in andere GEB's is opgenomen. Het aanmaken van het CST gebeurt op vertoon van het DEUCC van de betrokkene. Slechts beperkte informatie over de toepasbaarheid van het certificaat van de betrokkene zal een verwerking zijn van gegevens die niet door de betrokkene zelf werd voorgelegd, namelijk het gebruik van de Suspension list.
Maatregelen
De verschillende overheden hebben het belang van CST toegelicht en het toepassingsgebied ervan. Hierbij werd vooral gebruik gemaakt van berichtgeving in de pers als informatie die kan geconsulteerd worden via het internet. Bijkomend wordt de DPIA gepubliceerd die de verschillende verwerkingsverantwoordelijken aanduidt in de hele keten.
Residueel risico
Het residueel risico zal erin bestaan dat het toepassingsgebied van CST en de voorwaarden om een CST te bekomen veranderen in de tijd. Als de voorwaarden om een CST te bekomen gecontroleerd worden met informatie die niet rechtstreeks bij de betrokkene werd bekomen (bv. Validatieregels, suspension list), kan de

R25. Toelichten impact gegevensverwerking	
betrokkene moeilijkheden ondervinden wanneer het resultaat van de verwerking niet strookt met de opvatting van de betrokkene. (bv. Toegang geweigerd)	
Risicoscore	
Probabiliteit na maatregelen	2
Impact na maatregelen	2
Risico	MEDIUM

R26. Informatie over de dienst

R26. Informatie over de dienst
Kwetsbaarheid
Bestaande informatie die de dienst beschrijft is niet gemakkelijk toegankelijk voor de betrokkene, is niet gemakkelijk te begrijpen en / of vereist speciale kennis om het te begrijpen
Toelichting
De AVG voorziet dat de gebruiker in begrijpbare bewoordingen wordt geïnformeerd over de doelstellingen van CST, de verwerkingen die plaatsvinden en de gegevens die hiervoor gebruikt worden. De verwerking betreft hoofdzakelijk de interpretatie van de gegevens op het DEUCC van de burger.
Maatregelen
De burgers worden op volgende manier geïnformeerd: - De verwerkte informatie wordt opgesomd in de verschillende wetgevingen rond samenwerkingsakkoorden en de Europese verordening rond DEUCC. - De verschillende overheden hebben op hun webpagina's en via de pers de burger geïnformeerd over de verwerkingen die plaatsvinden. - Deze DPIA wordt gepubliceerd op de website van CovidScan.
Residueel risico
Het risico is net zoals bij R.25 dat de burger die zijn DEUCC aanbiedt niet op de hoogte is van veranderende voorwaarden om een DEUCC te genereren.

Risicoscore	
Probabiliteit na maatregelen	2
Impact na maatregelen	1
Risico	LAAG

R27. Informatie over aanvullende gegevens

R27. Informatie over aanvullende gegevens
Kwetsbaarheid
De betrokkene krijgt geen adequate informatie over waar gegevens vandaan komen, als ze niet direct van de betrokkene zijn verkregen
Toelichting
Artikel 14 van de AVG bepaalt de te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen. In het geval van deze toepassing worden er gegevens over PCR tests verwerkt wanneer een gebruiker zijn vaccinatiecertificaat presenteert
Maatregelen
De privacy notification van de CovidScan applicatie geeft de verwerking aan die gebeurt en wie de verwerkingsverantwoordelijke is. Externe bronnen zoals Suspension list dienen hier ook bij vermeld te worden. Deze DPIA die de gegevensverwerkingen in meer detail toelicht is gepubliceerd op de website.
Residueel risico

R27. Informatie over aanvullende gegevens	
De nodige meldingen in het wetgevend kader zijn voorzien zodat de kans dat de verwerkingsverantwoordelijke niet aan deze verplichting voldoet klein is.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R28. Informatie over derde dataverwerkers

R28. Informatie over derde dataverwerkers	
Kwetsbaarheid	
Er wordt geen informatie gegeven over relevante derden die ook de gegevens van de betrokkene ontvangen.	
Toelichting	
De wetgever voorziet een beperking van de verdere verwerking van gegevens uit CST. Deze mogen daarom niet aan derden doorgegeven worden.	
Maatregelen	
NVT	
Residueel risico	
NVT	
Risicoscore	
Probabiliteit na maatregelen	NVT
Impact na maatregelen	NVT
Risico	NVT

R29. Informering over gebruik van gegevens

R29. Informering over gebruik van gegevens
Kwetsbaarheid
Op het tijdstip van gegevensverzameling is de betrokkene niet of niet voldoende geïnformeerd over al het volgende: - de verantwoordelijke van de gegevensverwerking - het doel van de verwerking - wie de ontvangers van de gegevens - welke gegevens verplicht/facultatief zijn - het bestaan van het recht op toegang tot en het recht om de gegevens betreffende hem te corrigeren
Toelichting
Wanneer persoonsgegevens worden verzameld bij de betrokkene voorziet de AVG dat deze geïnformeerd wordt over bovenvermelde punten. Deze informatie is noodzakelijk opdat de betrokkene geïnformeerd kan beslissen om zijn instemming al dan niet te geven om de verwerking van zijn gegevens te laten gebeuren en de consequenties hiervan inschatten. Qua ontvangers en verwerkte gegevens heeft de wetgever reeds in een beperking van de verwerking voorzien en opgelgd welke gegevens kunnen verwerkt worden voor het genereren van een CST.
Maatregelen
Voor CovidScan werd een privacyverklaring opgesteld die voorziet in de nodige informatie. Bijkomend zijn de doelstelling van de app en de verschillende verantwoordelijken omschreven in het relevante KB en de daarmee verbonden samenwerkingsakkoorden. Deze DPIA die bijkomende informatie geeft staat gepubliceerd op de website van CovidScan

R29. Informering over gebruik van gegevens	
Residueel risico	
De kans blijft bestaan dat de informatie bepaalde groepen van de bevolking en de gebruikers niet zal bereiken doordat de informatie niet eenvoudig te begrijpen is. Door de beperking van de verwerking opgelegd door de wetgever in de samenwerkingsakkoorden is de impact beperkt.	
Risicoscore	
Probabiliteit na maatregelen	2
Impact na maatregelen	1
Risico	LAAG

R30. Geïndividualiseerde informatie over verwerkte gegevens

R30. Geïndividualiseerde informatie over verwerkte gegevens	
Kwetsbaarheid	
De betrokkene kan geen geïndividualiseerde informatie krijgen over welke gegevens over hem of haar worden verwerkt en waar de gegevens voor worden gebruikt.	
Toelichting	
Bij de verwerking van persoonsgegevens is het voorzien dat de betrokkene gepersonaliseerde informatie kan bekomen over de gegevens die verwerkt worden en die hem betreffen. De toepassing die gebruikt wordt is CovidScan. De verwerking gebeurt onmiddellijk en het resultaat wordt onmiddellijk aan de betrokkene meegedeeld. Om die reden is deze kwetsbaarheid niet verder in overweging genomen	
Maatregelen	
Niet van toepassing (NVT)	
Residueel risico	
Niet van toepassing.	
Risicoscore	
Probabiliteit na maatregelen	NVT
Impact na maatregelen	NVT
Risico	NVT

D09. Naleving van het recht op verbetering en verwijdering van persoonsgegevens

Principe	De betrokkene kan de gegevens corrigeren als er fouten in zitten of kan zijn/haar gegevens laten verwijderen
Samenvatting	In deze paragraaf moet worden bekeken hoe de organisatie zal omgaan met een verzoek om correctie van persoonlijke gegevens. Zijn er beperkingen? (bijvoorbeeld tekenlimieten in gegevensvelden of het ontbreken van de mogelijkheid om een vlag toe te voegen die aangeeft dat er relevante informatie in een fysiek bestand wordt bewaard)
Link AVG	Afdeling 3 Rectificatie en wissing van gegevens Artikel 16 Recht op rectificatie Artikel 17 Recht op gegevenswissing („recht op vergetelheid”)

R31. Wijzigen van gegevens

R31. Wijzigen van gegevens
Kwetsbaarheid
Er is geen procedure waarmee de betrokkene individuele gegevens kan verbeteren, wissen of blokkeren geïmplementeerd.
Toelichting

R31. Wijzigen van gegevens	
De behandelend arts van de betrokkene, de apotheker of het labo, dat de test uitvoert, verzenden in het kader van wettelijke regels inzake contactopsporing(gegevensbank I van het Samenwerkingsakkoord van 20 augustus 2020) een beperkt aantal persoonsgegevens van de betrokkene naar Sciensano. Evenzo is in het proces van de COVID19-vaccinatiecampagne voorzien dat de vaccinatiestatus naar de Vaccinnet+ databankverstuurd wordt. Sciensano en de betrokken gezondheidsadministratiesvan de regio's zullen deze informatie gebruiken om de nodige certificaten aan te maken. Conform artikel 16 AVG heeft de betrokkene de mogelijkheid deze gegevens te verbeteren. Voor de correctheid van de certificaten dient hiervoor bij de relevante verwerkingsverantwoordelijke de vraag voor eventuele correctie gesteld te worden. De relevante verwerking die in aanmerking kan komen voor vraag tot verbetering is de lijst met ID's van certificaten die geschorst zijn.	
Maatregelen	
De betrokkene van wie een DEUCC geweigerd wordt dient hiervoor de uitgever van het geweigerde certificaat te contacteren. De uitgever van het certificaat staat op het certificaat vermeld.	
Residueel risico	
De kans blijft bestaan dat een betrokkene niet op de hoogte is van de verwerking met de lijst met ID's van certificaten die geschorst zijn. Toch is probabiliteit beperkt omdat de betrokkene hierover geïnformeerd zou moeten zijn wanneer zijn certificaat ingetrokken is of wanneer een positieve COVID test werd afgelegd.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R32. Informeren over gewijzigde gegevens

R32. Informeren over gewijzigde gegevens	
Kwetsbaarheid	
De verantwoordelijke heeft geen procedure geïmplementeerd die relevante derde partijen op de hoogte brengt dat individuele gegevens zijn verbeterd, gewist of geblokkeerd.	
Toelichting	
De verwerking van gegevens voor het genereren van CST voorziet geen doorgifte aan derden. Om die reden wordt dit risico niet verder behandeld	
Maatregelen	
NVT	
Residueel risico	
NVT	
Risicoscore	
Probabiliteit na maatregelen	NVT
Impact na maatregelen	NVT
Risico	NVT

D10. Naleving van het recht op overdraagbaarheid van gegevens

Principe	De betrokkene moet op een eenvoudige manier van data verwerker kunnen veranderen
Samenvatting	De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen, en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder

	daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt
Link AVG	Artikel 20 Recht op overdraagbaarheid van gegevens

R33. Veranderen van verantwoordelijke

R33. Veranderen van verantwoordelijke	
Kwetsbaarheid	
De betrokkene kan niet van verantwoordelijke veranderen of moet zelf zijn eigen persoonsgegevens terug reconstrueren	
Toelichting	
De wetgever heeft de verwerkingsverantwoordelijke aangeduid bij middel van de verschillende samenwerkingsakkoorden. Het is niet voorzien dat een burger van aanbieder kan veranderen tenzij er een aanpassing is van zijn administratieve gegevens zoals deze verwerkt zijn in het rijksregister. Om die reden wordt dit risico niet verder behandeld.	
Maatregelen	
NVT	
Residueel risico	
NVT	
Risicoscore	
Probabiliteit na maatregelen	NVT
Impact na maatregelen	NVT
Risico	NVT

D11. Naleving van het recht op bezwaar

Principe	De betrokkene kan bezwaar aantekenen tegen de verwerking van zijn gegevens.
Samenvatting	De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens op basis van artikel 6, lid 1, onder e) of f), van artikel 6, lid 1, met inbegrip van profilering op basis van die bepalingen.
Link AVG	Artikel 21 Recht van bezwaar

R34. Bezwaar tegen beslissingsprocedures

R34. Bezwaar tegen beslissingsprocedures
Kwetsbaarheid
De betrokkene kan geen bezwaar maken tegen geautomatiseerde beslissingsprocedures die in het kader van de aangeboden service worden gebruikt.
Toelichting
AVG voorziet dat de betrokkene bezwaar kan uitoefenen tegen een verwerking van zijn persoonsgegevens. De verwerking van gegevens voor het genereren van een CST zijn vastgelegd in de wet bij middel van het samenwerkingsakkoord van 14 juli 2021. CST wordt gegenereerd wanneer aan de voorwaarden is voldaan. Omdat de controle dient te gebeuren met de CovidScan app dient ervan uitgegaan te worden dat de verwerking correct is gebeurd. De beslissing om al dan niet een CST te genereren is beschreven in de wettelijke voorwaarden om toegang te krijgen. Om die reden is een bezwaar in deze niet mogelijk en wordt het risico niet verder behandeld.
Maatregelen
Niet van toepassing
Residueel risico

R34. Bezwaar tegen beslissingsprocedures	
Niet van toepassing	
Risicoscore	
Probabiliteit na maatregelen	NVT
Impact na maatregelen	NVT
Risico	NVT

R35. Informeren doorgeven gegevens aan derden

R35. Informeren doorgeven gegevens aan derden	
Kwetsbaarheid	
De betrokkene is niet op de hoogte gesteld van het doorgeven van zijn gegevens aan derden of over het gebruik van zijn gegevens voor direct marketingdoeleinden	
Toelichting	
Het wettelijk kader voorziet dat verdere verwerking van gegevens niet toegestaan is, evenmin de doorgifte aan derden.	
Maatregelen	
NVT	
Residueel risico	
NVT	
Risicoscore	
Probabiliteit na maatregelen	NVT
Impact na maatregelen	NVT
Risico	NVT

R36. Bezwaar tegen verwerking van persoonsgegevens

R36. Bezwaar tegen verwerking van persoonsgegevens	
Kwetsbaarheid	
Er is geen procedure om bezwaar te maken tegen de verwerking van persoonsgegevens	
Toelichting	
AVG voorziet dat de betrokkene bezwaar kan uitoefenen tegen een verwerking van zijn persoonsgegevens. Voor het genereren van een CST dient de betrokkene zijn DEUCC te tonen. Deze handeling dient beschouwd te worden als een instemming om de gegevens te verwerken. Omdat er nadien geen verdere verwerking van de informatie meer plaatsvindt wordt dit risico niet verder behandeld. De verwerking van de gegevens in de Suspension list, is een uitvoering van de akkoorden van het laatste Uitvoerend samenwerkingsakkoord en is een verwerking opgelegd door de wet die dit Uitvoerend Samenwerkingsakkoord bekrachtigt.	
Maatregelen	
NVT	
Residueel risico	
NVT	
Risicoscore	
Probabiliteit na maatregelen	NVT
Impact na maatregelen	NVT
Risico	NVT

R37. Informeren over bezwaar verwerking van persoonsgegevens

R37. Informeren over bezwaar verwerking van persoonsgegevens
Kwetsbaarheid

R37. Informeren over bezwaar verwerking van persoonsgegevens	
De exploitant heeft geen procedure geïmplementeerd die relevante derde partijen op de hoogte brengt dat een betrokkene bezwaar heeft gemaakt tegen de verwerking van zijn persoonsgegevens.	
Toelichting	
Er is geen doorgifte aan derden voorzien. Om die reden is dit risico niet verder behandeld.	
Maatregelen	
NVT	
Residueel risico	
NVT	
Risicoscore	
Probabiliteit na maatregelen	NVT
Impact na maatregelen	NVT
Risico	NVT

D12. Naleving van de regeling in verband met geautomatiseerde individuele besluiten

Er worden individuele besluiten genomen die impact hebben op de betrokkene die zijn DEUCC ter beschikking stelt. De resultaten zijn ofwel het gevolg van de informatie verwerkt in het DEUCC, ofwel het resultaat van een controle wanneer een burger een certificaat aanbiedt dat geschorst is. Het enig toegestane middel om het DEUCC te controleren is de CovidScan app waardoor dit risico reeds verwerkt is in vorige beschouwingen.

D13. Naleven van de (technische) verplichtingen inzake opzet van de verwerking

Principe Voor het beschermen van de rechten van de betrokkenen dienen de verwerkingen te voorzien in voldoende veiligheidsmaatregelen.

Samenvatting Bij het ontwerpen van toepassingen die instaan voor het verwerken van persoonsgegevens zullen volgende maatregelen overwogen worden:

- Gegevensbescherming door ontwerp en door standaardinstellingen
- Bepaling rollen van de verwerkers
- Beveiliging van de verwerking wanneer personeel van de verwerkingsverantwoordelijke of de verwerker tussenkomt in de verwerking van de gegevens.

Link AVG Artikel 25
Artikel 26

R38. Privacy by design and by default

R38. Privacy by design and by default
Kwetsbaarheid
De gegevensverwerking is niet uitgewerkt volgens de principes van ontwerp en standaardinstellingen 'privacy by design and by default'.
Toelichting
De wetgever heeft voorzien welke de voorwaarden zijn om een CST te genereren vanaf DEUCC en hiervoor enkel toe te staan dat de CST module van de CovidScan app wordt gebruikt.
Maatregelen
Volgende maatregelen werden toegepast: - Verplicht gebruik van CovidScan app - Geen toestemming om gegevens op te slaan - Enkel de minimale informatie noodzakelijk om een persoon te identificeren en de beslissing te communiceren wordt verwerkt

R38. Privacy by design and by default	
- Bescherming van de lijst met ID's van vaccinatiecertificaten die tijdelijk geschorst zijn met een equivalentie van pseudonimisering	
Residueel risico	
Het principe van DPbD werd correct toegepast. De bestaande risico's werden eerder beschreven	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

D14. Naleven van organisatorische verplichtingen

R39. Bepaling van rollen van gegevensverwerkers

R39. Bepaling van rollen van gegevensverwerkers	
Kwetsbaarheid	
Geen duidelijke bepaling van de rollen van de gegevensverwerkers inzake de gegevensverwerking, waardoor het voor de betrokkene niet duidelijk is wie bevoegd is om de gegevens te raadplegen of te wijzigen	
Toelichting	
Het genereren van het CST gebeurt op basis van het DEUCC. Voor de verschillende mogelijke certificaten die een DEUCC kunnen vormen zijn verwerkingsverantwoordelijken aangeduid. Voor het genereren van het CST is de partij die de controle uitvoert de verwerkingsverantwoordelijke. Voor de lijst met ID's van certificaten die geschorst zijn, zijn de verwerkingsverantwoordelijken dezelfde als de verwerkingsverantwoordelijke voor het geschorste certificaat.	
Maatregelen	
De aanduiding van de verwerkingsverantwoordelijken is opgenomen in de privacy notification van CovidScan app	
Residueel risico	
Er werden geen bijkomende risico's m.b.t. dit punt vastgesteld	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R40. Gedragscodes of Certificeringsregelingen

R40. Gedragscodes of Certificeringsregelingen
Kwetsbaarheid
De verwerker beschikt niet over een goedgekeurde gedragscode of certificeringsregeling
Toelichting
De verwerkingsverantwoordelijke wordt geacht de veiligheid en het respect van de AVG door zijn verwerker in het kader van de vooropgestelde verwerkingen te controleren. Naast de instructies die de verwerkingsverantwoordelijke dient te geven, dient de organisatie van de verwerker ook te verzien in de nodige maatregelen die de garanties bieden dat de AVG gerespecteerd wordt. Voor het genereren van CST is er geen gebruik van een verwerker. Om die reden wordt dit risico niet verder behandeld.

R40. Gedragscodes of Certificeringsregelingen	
Maatregelen	
NVT	
Residueel risico	
NVT	
Risicoscore	
Probabiliteit na maatregelen	NVT
Impact na maatregelen	NVT
Risico	NVT

R41. Opleiding medewerkers

R41. Opleiding medewerkers	
Kwetsbaarheid	
De medewerkers zijn onvoldoende geïnformeerd over hoe om te gaan met de 'verwerking van persoonsgegevens'	
Toelichting	
Op het moment van genereren van een CST zal de verwerkingsverantwoordelijke beroep moeten doen op zijn medewerkers om de controle op CST op een juiste manier uit te voeren.	
Maatregelen	
Op de website “covidscan.be” is een handleiding voorzien om de CST te genereren.	
Residueel risico	
Het residuele risico kan zich voordoen wanneer de organisator van een event de handleiding niet consulteert en op foute manier de controle uitvoert.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

Besluit

De uitkomsten van de gegevensbeschermingseffectbeoordeling geven aan dat er geen hoge risico’s bestaan voor de betrokkenen wanneer de CST gegenereerd wordt met de middelen die door de overheid ter beschikking worden gesteld.
Er blijft een beperkt aantal risico’s over van het niveau MEDIUM.