Contactopsporingsapplicatie 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.
API	Application Programming Interface. Deze interface zorgt ervoor dat software kan communiceren met standaard softwarepakketten.
Autorisatiecode	De anonieme autorisatiecode die de Gegevensbank VI aanmaakt om de gebruiker die positief getest is toe te laten beveiligde sleutels op te laden in Gegevensbank V.
AVG	De Algemene verordening gegevensbescherming (AVG) (Engels: General Data Protection Regulation (GDPR) 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.
Beveiligde sleutel	Een beveiligde sleutel die na installatie van de app elke dag wordt gegenereerd en opgeslagen op de smartphone waarop de app is geïnstalleerd. Deze sleutel wordt Temporary Exposure Key (TEK) genoemd in de documentatie van Apple en Google.
Betrokkene	De geïdentificeerde of identificeerbare persoon van wie zijn of haar gegevens worden verwerkt.
Contact	Voor contactonderzoek is een contact een gebruiker die participeerde in een interactie met een gebruiker die positief testte op het virus, en waarbij de duur en de afstand een groot risico betreft op besmetting.
Content Delivery Network (CDN)	Een content delivery network, oftewel een contentdistributienetwerk (CDN), is een geografisch gedistribueerd netwerk van proxyservers die informatie van een centraal punt aanbieden aan de eindgebruikers van die informatie. Het doel is om hoge beschikbaarheid en prestaties te bieden door de dienst ruimtelijk te distribueren ten opzichte van de eindgebruikers.
CTPC code	De corona test prescription code is een code die per SMS wordt opgestuurd door het call center naar personen die moeten

	worden getest op besmetting met COVID-19, De corona test prescription code is steeds een code van 16 alfanumerieke posities.
DP-3T (=Distributed Privacy-Preserving Proximity Tracking)	Een open-bron systeem dat naar aanleiding van de COVID-19 uitgewerkt werd door een pan-Europese groep van academici gespecialiseerd in onder meer encryptie, informatiebeveiliging, privacy en epidemiologie met als doel digitale contactopsporing te faciliteren.
Gegevensbank V	De Gegevensbank V bedoeld in het koninklijk besluit nr. 44 die de loggegevens van de verschillende gebruikers ontvangt en die later via CDN verdeeld worden.
Gegevensbank VI	Een gegevensbank waarvoor Sciensano de verwerkingsverantwoordelijke is en waarin zeer tijdelijk de testresultaten worden opgeslagen, samen met de testcode, de datum van staalafname en de datum waarop de gebruiker besmettelijk is geworden overeenkomstig het proces beschreven in artikel 2, § 1, 3° van het uitvoerings-KB.
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	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.
Instemming, instemmen met	Een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling: a) een voorgestelde verwerking op zijn gegevens goedkeurt,

	b) een dienstverlening waarbij zijn gegevens verwerkt kunnen worden aanvaard of c) instemt met het doorsturen van gegevens op zijn toestel na een dienst in het netwerk zoals vermeld in artikel 129 van de wet elektroniche communicatie. Instemming valt in deze context niet te verwarren met de rechtsgrond "toestemming" voor gegevens-verwerking zoals bepaald in art. 6 §1 van de AVG.
Koninklijk besluit nr. 44	Het koninklijk besluit nr. 44 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden 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.
Manuele contactopsporing	Bij manuele contactopvolging worden personen die in contact stonden met een persoon die (vermoedelijk) besmet is met Covid-19 opgespoord aan de hand van telefonische of face-to-face interviews door geautoriseerde actoren (bv. gezondheidsinspecteurs).
Niet-gepersonaliseerd tijdelijk serienummer	Willekeurige combinatie van enen en nullen, die door een smartphone waarop de app is geïnstalleerd via een Bluetooth baken wordt uitgezonden en die bestaat uit een willekeurig getal en de vercijfering van anonieme gegevens van de smartphone.
INSZ nummers	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.

Risicocontact	Een contact gedurende minstens 15 minuten binnen afstand van minder dan 2 meter met een besmet persoon; dat contact wordt vastgesteld wanneer op een smartphone een niet-gepersonaliseerd tijdelijk serienummer wordt gevonden dat overeenkomt met een niet-gepersonaliseerd serienummer dat werd uitgezonden door de smartphone van een besmette gebruiker.
Samenwerkingsakkoord	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.
Testcode	Een code die bestaat uit willekeurige cijfers en wordt aangemaakt door de app bij de aanvraag van een test.
Uitvoerend samenwerkingsakkoord	Uitvoerend samenwerkingsakkoord van 13 oktober 2020 tussen de Federale staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie, betreffende de digitale contactopsporingsapplicatie(s), overeenkomstig artikel 92bis, §1, derde lid, van de Bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.
Uitvoerings-KB	Koninklijk besluit van 17 september 2020 tot uitvoering van het koninklijk besluit nr. 44 van 26 juni 2020 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden 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.
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.

Algemeen kader

Op 11 maart 2020 heeft de Wereldgezondheidsorganisatie (WHO) het SARS-CoV- 2-virus uitgeroepen tot een pandemie. Het SARS-CoV-2-virus is een zeer besmettelijk virus dat de ziekte COVID-19 veroorzaakt, die voornamelijk voor ouderen en personen met een medische voorgeschiedenis ernstige medische problemen veroorzaakt of dodelijk kan zijn.

Ook België blijft niet gespaard van deze pandemie en in het kader van de COVID-19-gezondheidscrisis en om een verdere verspreiding van de ziekte COVID- 19 tegen te gaan, werd daarom een Nationale Veiligheidsraad opgericht, waarin de vertegenwoordigers van de federale overheid en de deelstaten overleg plegen om op elkaar afgestemde maatregelen te nemen teneinde de verdere verspreiding van COVID-19 te beperken.

In de loop van de maanden maart en april 2020 werden zowel door de federale overheid als door de deelstatelijke regeringen al verschillende maatregelen genomen om een verdere verspreiding van COVID-19 tegen te gaan. Die genomen maatregelen hadden voornamelijk tot doel om fysieke contacten tussen personen te minimaliseren tot het noodzakelijke, om op die manier de verspreiding van COVID-19 in tegen te gaan (de zogenoemde 'lock-down light').

De COVID-19-crisis is daarna een nieuwe fase ingegaan, waarbij het aantal ziekenhuisopnames en het aantal sterftegevallen door COVID-19 een dalende trend aannam. Om die reden had de Nationale Veiligheidsraad op 24 april 2020, na advies van de Groep van Experten belast met de Exit-Strategie (GEES) een plan opgesteld waarin de toegelaten fysieke contacten tussen de personen geleidelijk aan versoepeld worden en de 'lockdown light' wordt afgebouwd (de 'exitstrategie').

Het versoepelen van de maatregelen, waardoor er opnieuw meer fysiek contact tussen personen zal zijn, brengt uiteraard ook een risico met zich mee dat het aantal gevallen van COVID-19 opnieuw kan toenemen. Zo getuige ook de start van een zogenaamde tweede golf in juli 2020. Het is dus noodzakelijk dat in fases van versoepeling de nodige maatregelen worden genomen om een verdere verspreiding van COVID-19 tegen te gaan.

Een van die maatregelen is het vroegtijdig opsporen van personen die besmet zijn met COVID-19, of waarvan er een vermoeden bestaat dat zij besmet zijn met COVID-19, om aan deze personen de nodige aanbevelingen te kunnen geven (thuisisolatie, telewerken enzovoort) om te vermijden dat deze personen andere personen zouden besmetten met het SARS-CoV-2-virus.

Gezien de besmettelijkheid van het SARS-CoV-2-virus, is het aangewezen om personen waarmee de besmette of vermoedelijk besmette persoon in contact is geweest te kunnen detecteren ('contactopsporing'). Op deze manier kunnen aan deze personen de nodige aanbevelingen worden gegeven (zich laten testen, contacten beperken enzovoort) om een verdere verspreiding van COVID-19 te voorkomen.

Sinds het SARS-CoV-2-virus zich begin 2020 over heel Europa begon te verspreiden, zijn de publieke en politieke debatten steeds meer gericht op een technologische oplossing voor dit meest urgente probleem.

Kan een app voor contactopsporing op ieders smartphone bijdragen om de pandemie in te dammen? Deze systemen zouden automatisch de interpersoonlijke contacten van alle gebruikers registreren en het zo mogelijk maken om de infectieketens snel te traceren. Vervolgens kunnen potentieel blootgestelde personen efficiënt worden getraceerd om ze in een vroeg stadium van de infectie hiervan te verwittigen en zo te zich te laten isoleren.

De Gegevensbeschermingsautoriteit (GBA) benadrukt in zijn advies dat elke opsporingsapplicatie moet voldoen aan de regels en specificaties die zijn vastgesteld door de EDPB (European Data Protection Board), dat hierover richtsnoeren en een "toolbox" heeft gepubliceerd die gebruikt werd bij de aanpak van het veiligheidsvraagstuk en de opmaak van deze gegevensbeschermingseffectenbeoordeling.

In België is er eerst gekozen voor manueel contactonderzoek zoals het tot op heden met andere infectieziekten ook werd ingericht. Aangezien vervolgens beslist is geweest om een contactopsporingsapplicatie te ondersteunen is de opmaak van deze bijkomende gegevensbeschermingseffectenbeoordeling noodzakelijk.

Introductie

Voor een goed begrip van deze gegevensbeschermingseffectbeoordeling is het belangrijk om vooreerst een beknopt beeld te schetsen van de betrokken platformen en gegevensverwerkingen. Een meer gedetailleerde beschrijving van de architectuur en de gegevensstromen volgt later (zie punt 2.3.).

Het systeem voor digitale contactopsporing bestaat enerzijds uit een mobiele applicatie die de gebruiker (een burger) vrijwillig op zijn telefoontoestel *(GSM, smartphone)* kan installeren en gebruiken. Via een correcte activatie van de app kan een gebruiker met behulp van Bluetooth niet-gepersonaliseerde tijdelijke serienummers (oftewel geheime ID's) uitwisselen met andere app-gebruikers waarmee hij in nabij contact komt. Deze niet-gepersonaliseerde tijdelijke serienummers worden tijdelijk bewaard in de app om in geval van besmetting waarschuwingsacties te kunnen ondernemen. Daarnaast bevat het systeem een bijhorende serverinfrastructuur die het opvragen van een persoonlijk testresultaat en het anoniem versturen van waarschuwingen naar risico-contacten van een persoon met een positieve labotest faciliteert.

De serverinfrastructuur bestaat uit twee gegevensbanken (oftewel databases in het Engels, afgekort DB). Het betreft de volgende twee gegevensbanken.

- **De testresultaten-gegevensbank (=Gegevensbank VI):** Een gegevensbank om de resultaten van de uitgevoerde COVID-19 labotest uit te wisselen met de gebruiker van de applicatie en hem te voorzien van een testcode. De testcode is noodzakelijk voor betrouwbare communicatie over besmettingen met de centrale gegevensbank.
- **De centrale gegevensbank met loglijst van de opsporingsapplicatie (=Gegevensbank V):** een gegevensbank voor de uitwisseling van de beveiligde sleutels om andere burgers te waarschuwen dat ze in contact kwamen met een besmette persoon. In het geval van een bevestigde besmetting kan de gebruiker ervoor kiezen om zijn lijst met beveiligde sleutels

representatief voor de dagen waarop de gebruiker besmettelijk was te delen met de centrale gegevensbank.

Er zijn met andere woorden twee platformen waar gegevens verwerkt kunnen worden: 1) een mobiele applicatie en 2) een serverinfrastructuur met gegevensbanken. Zoals verder zal blijken, behoudt de gebruiker van het toestel autonomie. Hij/zij beslist namelijk zelf over de installatie en gebruik van de applicatie alsook over het al dan niet uitwisselen van gegevens met de serverinfrastructuur. De gebruiker heeft ook steeds de mogelijkheid om de applicatie tijdelijk uit te schakelen zonder daarvoor de Bluetooth van het toestel uit te schakelen.

Tabel 1. Overzicht platformen en gegevensverwerkingen

	App *(= aangeboden door de deelstaten, vrijwillig beheer door de gebruiker)*	Centraal platform *(= server-infrastructuur beheerd door Sciensano)*
Uitwisselen contacten	-Aanmaken beveiligde sleutels -Aanmaken niet-gepersonaliseerd tijdelijk serienummer -Versturen van niet-gepersonaliseerd tijdelijk serienummer -Ontvangen van Bluetooth tokens en stockeren ervan met bijkomende gegevens	
Aanvraag COVID testing	-Aanmaken testcode R1 -Polling van gegevensbank voor resultaten -Opladen van relevante beveiligde sleutels naar centrale gegevensbank	-Beschikbaar maken resultaten COVID test -Verwijderen resultaten -Aanmaken autorisatiecode -Ontvangen beveiligde sleutels
Contactopsporing	-Downloaden beveiligde sleutels van besmettelijke personen -Berekenen van risicocontacten o.b.v ontvangen beveiligde sleutels en geregistreerde niet-gepersonaliseerde tijdelijke serienummers in relatie tot duur en afstand van de contacten	-Verdelen van beveiligde sleutels via CDN

Deze gegevensbeschermingseffectbeoordeling maakt omwille van coherentie gebruik van dezelfde terminologie als het juridische kader voor contactopsporing. Dit juridische kader reguleert zowel de gegevensbanken van manuele contactopsporing als de gegevensbanken van digitale contactopsporing. Het gaat daarbij in totaal over zes gegevensbanken gedefinieerd per nummer (voor meer details zie definities in KB nr. 44, het Samenwerkingsakkoord, het uitvoerings-KB en het uitvoerend Samenwerkingsakkoord). Zoals aangehaald, maken enkel gegevensbank V en gegevensbank VI deel uit van de contactopsporingsapplicatie. Hierbij als achtergrondinformatie een beknopte beschrijving van de andere vier gegevensbanken opgericht voor de organisatie van de manuele contactopsporing:

- Gegevensbank I met contact- en gezondheidsgegevens van personen met een (vermoede) besmetting meegedeeld door de ziekenhuizen, labo's, de huisartsen en de medewerkers van het contactcenter. Het betreft een centrale gegevensbank beheerd door Sciensano die gegevensbank II, III en VI voedt.
- Gegevensbank II van Sciensano met gepseudonimiseerde gegevens voor epidemiologisch onderzoek inzake de verspreiding van COVID-19.

- Gegevensbank III van de deelstaten met belorders voor de medewerkers van het contactcentrum van de deelstaten.
- Gegevensbank IV van de deelstaten met contactgegevens van artsen of administratief verantwoordelijken van collectiviteiten (bv. scholen, kinderdagverblijven, werkplaatsen, …) om hen te informeren over besmettingsrisico's.

Hoewel in éénzelfde juridisch kader opgenomen, is het belangrijk om te vermelden dat er strikte scheidingen zijn inzake het beheer van deze aparte gegevensbanken.

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

De Belgische opsporingsapplicatie en bijhorende serverinfrastructuur bieden ondersteuning voor communicatie inzake besmettingen *(o.a. resultaten labotesten)*, gezondheidsrisico's *(nabije contacten met een persoon met COVID-19)* en preventiemaatregelen ter bestrijding van de verspreiding COVID-19 *(bv. quarantaine).*

Gelet op

- artikel 35 van de AVG,
- de lijst van het soort verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling (afgekort GEB) steeds verplicht is zoals vastgelegd door de Belgische Gegevensbeschermingsautoriteit en de Vlaamse Toezichtcommissie,
- de Sciensano Standard Operating Procedure (SOP) I/00/24/N Data Protection Impact Assessment 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 de architectuur van de opsporingsapplicatie een GEB vereist.

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

- De architectuur van het systeem voor digitale contactopsporing laat een grootschalige verwerking van een bijzondere categorie van persoonsgegevens, met name gezondheidsgegevens, toe. Het gaat daarbij over gegevens gerelateerd aan besmettingen en/of risico's inzake besmettingen met het coronavirus COVID-19 (zie 2.2.). De app wordt vrijwillig aangeboden aan alle inwoners van België met een smartphone. Opgelet: 'Grootschaligheid' is evenwel afhankelijk van het aantal gebruikers van de applicatie alsook het aantal besmettingen.
- De opsporingsapplicatie heeft de ambitie om laagdrempelig te zijn. Iedere Belgische inwoner, vanaf 13 jaar, die in het bezit is van een smartphone zou in principe de mogelijkheid moeten hebben om indien gewenst de opsporingsapplicatie op zijn/haar smartphone te installeren en gegevens uit te wisselen. Het gaat daarbij ook over kwetsbare personen zoals kinderen (vanaf 13 jaar), werknemers, geesteszieken, asielzoekers, bejaarden, …
- Er wordt Cloud technologie gebruikt bij de verwerking. De serverinfrastructuur maakt namelijk gebruik van AWS Cloud Services om gegevens tijdelijk te bewaren.
- Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen : inzetten van bluetooth technologie om nabijheid van andere personen te berekenen in het kader van het identificeren van risicovolle contacten.

Deze GEB heeft geen betrekking op de gegevensverwerkingen voor manuele contactopsporing via de callcentra, de gezondheidsinspecteurs en mobiele teams van de deelstaten.

Sectie II: Beschrijving van de gegevensverwerkingen

2.1. Persoonsgegevens

De personen van wie gegevens verwerkt worden, zijn gebruikers van de contactopsporingsapplicatie Het gaat over burgers die deze app vrijwillig op hun smartphone downloaden en activeren. Afhankelijk van de verwerking en het verwerkingsplatform kunnen zij verschillende hoedanigheden aannemen: bijvoorbeeld

- Persoon die in de nabijheid van een andere applicatiegebruiker komt en daardoor Bluetooth signalen opvangt die tijdelijk door de app geregistreerd worden.
- Persoon die een COVID-19 labotest laat uitvoeren door een arts en het resultaat van de test via zijn app opvraagt.
- Persoon die het positieve testresultaat en een loglijst via zijn app naar een centrale gegevensbank verzendt om andere personen waarmee hij in contact kwam voor besmettingsrisico's te waarschuwen. Bij het verwerken van de gegevens zijn deze op een zodanige manier gepseudonimiseerd dat de ontvanger quasi niet kan achterhalen wie de besmette persoon is.
- Persoon die via zijn app een waarschuwing krijgt dat hij/zij in contact kwam met een besmet persoon alsook instructies voor acties (bv. het laten uitvoeren van een test, zelfisolatie, doktersbezoek).

Het type gegevens zijn gepseudonimiseerde identificatiegegevens en indien van toepassing gezondheidsgegevens en gegevens over verblijf in het buitenland.

Gepseudonimiseerde identificatiegegevens

Een digitale contactopsporingsapplicatie op basis van het DP-3T systeem slaat enkel gepseudonimiseerde gegevens op, op het toestel van de gebruiker, met name beveiligde sleutels en niet-gepersonaliseerde tijdelijke serienummers, zonder verwijzing naar de identiteit van de personen met wie het contact heeft plaatsgevonden, noch naar de plaats waar het contact heeft plaatsgevonden. De datum waarop het contact heeft plaatsgevonden wordt wel bewaard omdat dit nodig is om te kunnen vaststellen of het contact heeft plaatsgevonden tussen het begin van de besmettelijkheid en de vaststelling van de besmetting.

Technisch gezien zou men kunnen stellen dat de beveiligde sleutels die gebruikt worden op het toestel van de gebruiker en eigen zijn aan een gebruiker, alsnog (en enkel door gebruik te maken van hacking technieken) zouden kunnen toelaten om de gedeelde serienummers van diezelfde gebruiker te ontsleutelen en terug te koppelen aan die gebruiker. Dus hoewel eerder theoretisch van aard, bestaat er dus nog een sleutel, vandaar dat de gegevens eerder als gepseudonimiseerd moeten beschouwd worden, dan geanonimiseerd. De toegang tot deze beveiligde sleutels is afgeschermd, ook voor de gebruiker. Enkel met toegang tot het toestel en de nodige hacking technieken zou men eventueel in staat kunnen zijn om de sleutel te achterhalen. Het enige wat daar dan nog uit zou kunnen geleerd worden, is of de gebruiker zich gemeld heeft als besmette gebruiker of niet. Centraal kan er echter

niets ontsleuteld worden. Ook andere gebruikers kunnen op geen enkele manier de gedeelde serienummers terugkoppelen aan een individu.

Gezondheidsgegevens

Indien een gebruiker van de applicatie een COVID-19 labotest laat uitvoeren (of voor COVID-19 symptomen op consultatie bij een arts gaat) en het resultaat via zijn app wil ontvangen, zullen volgende gegevens verwerkt worden:

- Testcode
- Vermoedelijke datum waarop de gebruiker besmettelijk is geworden
- Datum afname labotest COVID-19 (of consultatie)
- Resultaat labo-test
- Corona Test Prescription Code (= CTPC code)
- Sterk vermoeden van besmetting door de arts (ondanks negatieve labotest of bij onmogelijkheid om een test uit te voeren)

Meerdere van deze variabelen worden nu reeds door artsen en labo's verplicht geregistreerd in het kader van manuele contactopsporing waarbij het contactcentrum van de deelstaten dergelijke gegevens gebruikt om hun belorders of veldbezoeken te organiseren.[1] De variabelen testcode en vermoedelijke datum waarop de gebruiker besmettelijk is geworden worden voor gebruikers van de opsporingsapplicatie toegevoegd in de bestaande registratiesystemen van artsen om op die manier bepaalde functies van de applicatie te ondersteunen (zie 2.3.2.).

In het kader van administratieve vereenvoudiging voor zorgverleners en situaties waarbij een persoon zich via een CPTC code rechtstreeks tot een triage- of afnamecentrum kan wenden, hebben app-gebruikers ook de mogelijk om de testcode en vermoedelijke besmettingsdatum zelf door te geven via een webformulier op www.coronalert.be.

Gegevens over verblijf in het buitenland: landen EER

Een gebruiker die besmet is en die personen waarmee hij in nabij contact kwam wil waarschuwen, heeft de mogelijkheid om landen van Europese Economische Ruimte (EER) waar hij/zij tijdens de besmetting verbleef mee te delen zodat interactie met opsporingsapplicaties van die landen mogelijk is.

2.2. 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

[1] Voor meer informatie over gegevensverwerkingen manuele contact tracing: zie
-Privacyverklaring:
https://www.sciensano.be/sites/default/files/20200701_kennisgeving_burgers_centrale_database_sciensano_v4_nl.pdf
-Website: https://covid19lab.healthdata.be/

gegevensbeschermingsprincipes op vlak van gezondheidsgegevens en het implementeren van methoden van beveiliging en pseudonimisering van gegevens

Zoals bepaald in Koninklijk besluit nr. 44 en het Samenwerkingsakkoord[2] is Sciensano verwerkingsverantwoordelijke voor de gegevensbank met de centrale loglijst van de opsporingsapplicatie (Gegevensbank V). Naast de gegevensbank met de centrale loglijst is Sciensano tevens verwerkingsverantwoordelijke voor de testresultaten-gegevensbank (gegevensbank VI) waarvoor zij een beperkt aantal gegevens aanlevert via zijn bestaande databank voor manuele contactopsporing (gegevensbank I).

De Sciensano dienst healthdata.be staat in voor beheer van vermelde gegevensbanken. Deze dienst met opdrachten inzake technische facilitering van (gezondheids)gegevensbanken staat los van de Sciensano diensten belast met epidemiologische onderzoek. Sciensano ziet erop toe dat er geen kruising gebeurt met de andere databanken die zij beheert.[3]

(Gezondheids)administraties van de deelstaten

Gelet op bevoegdheidsverdelende regels inzake preventieve gezondheidszorg bepaalt art. 14 § 3 van het Samenwerkingsakkoorddat de deelstaten verantwoordelijk zijn voor de terbeschikkingstelling van de contactopsporingsapplicatie.

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 Diensten van het Verenigd College van 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.

De administraties van de deelstaten richten in het kader van manuele contactopsporing ook callcentra in. De callcentra zullen door burgers gebeld kunnen worden voor het verkrijgen van een covicode waarmee ze een positief testresultaat aan hun app kunnen koppelen. Voor meer informatie: zie 2.3.4. van deze GEB.

[2] *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 regionale overhedengefedereerde 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.*

[3] Zie onder andere ook de algemene toelichting KB nr. 44 omtrent gegevensbank V: "Sciensano moet er op toezien dat de nodige technische en organisatorische maatregelen genomen zijn om de loglijst te beschermen, en dat de gegevens van de loglijst niet gekruist worden met andere databanken."

Onderaannemers

Voor de ontwikkeling, de inproductiestelling, het onderhoud en support-activiteiten van de app en de backoffice van de opsporingsapplicatie werd er een lastenboek uitgegeven: https://www.corona-tracking.info/wp-content/uploads/2020/07/Smals-BB-001-031-2020.pdf

- De opdracht werd door de deelstaten gegund aan de firma DEVSIDE ingeschreven in de Kruispuntbank van Ondernemingen onder het nummer 0892.864.907, waarvan de kantoren gelegen zijn te J.F. Debeckerlaan 107, 1200 Sint-Lambrechts-Woluwe met als onderaannemer IXOR ingeschreven in de Kruispuntbank van Ondernemingen onder het nummer 0478.493.179, waarvan de kantoren gelegen zijn te Schuttersvest 75, 2800 Mechelen.

Voor de serverinfrastructuur zal Sciensano in het kader van de opsporingsapplicatie beroep doen op de AWS Cloud van Amazon via de leverancier SoftwareONE, ingeschreven in de Kruispuntbank van Ondernemingen onder het nummer BE 0844.127.058, waarvan de kantoren gelegen zijn te Esplanade 1 box 3, Suite 315, 1020 Brussel. Amazon en hun leverancier zullen als verwerker in opdracht van Sciensano tijdelijk gegevens bewaren.

Voor een SMS-systeem en het webformulier gericht op de uitwisseling van CTPC codes en testcodes voor ontvangst van een labotestresultaat in de app wordt er gebruik gemaakt van dienstverlening van Smals, een vzw gevestigd in de Fonsnylaan 20 te 1060 Brussel. Smals is een verwerker van Sciensano in het kader van Gegevensbank I die de testresultatenserver van de app (=Gegevensbank VI) voedt.

Wat de callcenters betreft die burgers kunnen helpen bij het verkrijgen van een covicode om een positief testresultaat zelf te kunnen koppelen aan hun app doen de betrokken administraties van de deelstaten beroep op de volgende partijen.

Vlaams Agentschap Zorg & Gezondheid:

- De groep Koramic2Engage, met de zusterbedrijven IPG Contact Solutions, in2com, Call-IT)
- N-Allo
- Callexcell
- Yource
- ZPG Intermut

Agence Wallonne pour une Vie de Qualité (AVIQ)

- GAP Intermut
- IKanbi
- Call Excell
- Entra & LEM Intérim

De Diensten van het Verenigd College van de Gemeenschappelijke Gemeenschapscommissie (GGC):

- N-Allo

Het Ministerium der Deutschsprachigen Gemeinschaft (MDG) doet geen beroep op een onderaannemer voor hun callcenter.

Huisartsen, ziekenhuisartsen en artsen werkzaam binnen triageposten

In het kader van de werking van de contactopsporingsapplicatie zullen artsen naast de verplichte registraties in het kader van manuele contactopsporing bijkomende gegevens registreren en meedelen via de bestaande kanalen (o.a. eForms)[4] naar Sciensano. De bijkomende gegevens zijn een testcode en vermoedelijke datum van besmetting.

Apple en Google

Kandidaat-gebruikers van de contactopsporingsapplicatie dienen, afhankelijk van het type smartphone waarvan gebruik wordt gemaakt, deze te downloaden uit de Apple App Store (iOS) of Google Play Store (Android). Beide downloadomgevingen zijn publiek beschikbaar.

Apple en Google ontwikkelden een API om zo de ontwikkeling van contactopsporingsapplicaties op basis van het DP-3T protocol mogelijk te maken alsook te laten functioneren op hun besturingssystemen (IOS resp. Android). Het ontwerp van de API en het systeem waarvan de API onderdeel uitmaakt verhindert dat Apple en Google toegang krijgen tot gegevens over de gebruikers. Zie ook de nota "Exposure Notification. Frequently Asked Questions" van Apple en Google: *"In keeping with our privacy guidelines, Apple and Google will not receive identifying information about the user, location data, or information about any other devices the user has been in proximity of."*

https://blog.google/documents/73/Exposure_Notification_-_FAQ_v1.1.pdf

Om het gebruik van de van de "Exposure Notification API" van Google en Apple te faciliteren kan dit het gebruik van onderliggende lagen van het besturingssysteem noodzaken. Zo zal bv. bij Android de API steunen op "Google Play Services" die aan de contact tracing app, net zoals aan andere apps op het toestel, een aantal basisdiensten zal leveren. Bij het gebruik van deze diensten zal Google gegevens verzamelen betreffende het toestel, toepassingen, locatie en diensten. De verwerking van deze gegevens maken strikt genomen geen deel uit van de verwerkingen van de contactopsporingsapplicatie en vallen onder een toestemming die de gebruiker gegeven heeft bij het configureren van zijn google account of bij het indienststellen van zijn toestel. Het valt op te merken dat de verzamelde gegevens geen inhoudelijke gegevens van de contactactopsporingsapplicatie bevatten.

Europese Commissie en betrokken gezondheidsautoriteiten van EER lidstaten

De lidstaten van de Europese Commissie hebben een akkoord bereikt om de uitwisseling van gegevens tussen nationale contactopsporingsapplicaties mogelijk te maken. Bijgevolg kunnen burgers die gebruik maken van de Belgische contactopsporingsapplicatie ook tijdens of na een verblijf in een ander land van de Economische Europese Ruimte waar ook de DP3T technologie gebruikt wordt, contacten detecteren en in geval van besmetting deze contacten waarschuwen. De Europese Commissie biedt daarvoor een federatieve gateway aan. Deze gateway bestaat uit een beveiligde IT-infrastructuur die voorziet in een gemeenschappelijke interface waar gezondheidsautoriteiten van landen van de Europese Economische Ruimte een minimale verzameling gegevens kunnen uitwisselen (zie 2.3.3.).

[4] Voor meer info: zie Beraadslaging nr. 20/132 van 3 mei 2020, gewijzigd op 13 mei 2020, 2 juni 2020, 7 juli 2020, 31 juli 2020, 3 november 2020 en 30 maart 2021 van het Informatieveiligheidscomité Sociale Zekerheid & Gezondheid betreffende de mededeling van persoonsgegevens door diverse zorgverleners of organisaties in de gezondheid of de zorg aan Sciensano en de verdere mededeling ervan in het kader van de strijd tegen de verspreiding van het coronavirus sars-cov-2

De Commissie, als aanbieder van technische en organisatorische oplossingen voor de federatieve gateway, verwerkt gepseudonimiseerde persoonsgegevens namens de betrokken gezondheidsautoriteiten van lidstaten die als gezamenlijke verwerkingsverantwoordelijken deelnemen aan de federatieve gateway en is derhalve een verwerker. Deze rollen worden beschreven in artikel 7 bis van het *Uitvoeringsbesluit (EU) 2020/1023 van de Commissie van 15 juli 2020 tot wijziging van Uitvoeringsbesluit (EU) 2019/1765 wat betreft de grensoverschrijdende uitwisseling van gegevens tussen nationale mobiele applicaties voor het traceren en waarschuwen van contacten met het oog op de bestrijding van de COVID-19-pandemie).* Een lijst met de namen en contactgegevens van de verwerkingsverantwoordelijk per deelnemende lidstaat is beschikbaar op volgende website: https://ec.europa.eu/health/ehealth/covid-19_nl. Deze lijst zal worden aangevuld naarmate er meer lidstaten toetreden. Voor toetreding dient een lidstaat de nodige documentatie aan te leveren waaruit onder andere blijkt dat er voor hun app een rechtsgrond, een privacyverklaring en gegevensbeschermingseffectbeoordeling bestaat. België verkreeg eind november 2020 groen licht om de technische werkzaamheden inzake toetreding tot de gateway op te starten. Hierbij hoopt België eind december 2020/begin januari 2021 live te kunnen gaan.

2.3. Gegevensverwerkingen

In dit onderdeel volgt een stapsgewijze beschrijving en illustratie van de gegevensverwerkingen.

2.3.1. Gegevensverwerkingen bij contacten met andere burger

De burger heeft de contactopsporingsapplicatie oftewel de 'Coronalert App' succesvol geïnstalleerd op zijn telefoon en alle instellingen geactiveerd voor een goede werking van de app. Vanaf dat moment is in de achtergrond de module "blootstellingsmeldingen voor COVID-19[5]" (ook gekend als exposure logging) in combinatie met de app actief. Opgelet: Deze module, kan indien gewenst door de gebruiker, tijdelijk uitgeschakeld worden (zonder dat daarvoor de Bluetooth op het toestel moet uitgeschakeld worden. (Zie ook de activatieschermen van de app in de bijhorende presentatie).

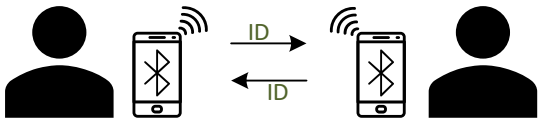
Volgende acties worden uitgevoerd in de achtergrond:

- elke dag maakt de app een nieuwe tijdelijke beveiligde sleutel[6] (TEK / Temporary Exposure Key) aan, en bewaart deze op het telefoontoestel voor een periode van 14 dagen samen met de datum
- iedere 10 minuten maakt de app op basis van de beveiligde sleutel een niet-gepersonaliseerd tijdelijk serienummer[7] aan
- iedere 0,5 seconde zendt het toestel via Bluetooth het niet-gepersonaliseerde tijdelijke serienummer (Bluetooth-tokens) uit naar andere smartphones in de buurt die gebruik maken van de Coronalert App
- ieder toestel met een notificatie app vangt iedere 5 minuten gedurende 4 seconden de uitgezonden niet-gepersonaliseerde tijdelijke serienummers op en bewaart deze op de

[5] De blootstellingsmeldingen voor COVID-19 zijn terug te vinden onder de instellingen van de telefoon. Voor Android: Instellingen > Google-instellingen > Blootstellingsmeldingen voor COVID-19, voor iOS: Instellingen > Privacy > Gezondheid óf Bluetooth > Blootstelling aan COVID-19.
[6] Willekeurige tekst (tekst en cijfers) van 128 bits
[7] Willekeurig nummer van 128 bits

telefoon voor een periode van 14 dagen samen met de datum en de sterkte van het Bluetooth-signaal

Schema uitwisseling niet-gepersonaliseerde tijdelijke serienummers:



Schema lijst met verstuurde en ontvangen niet-gepersonaliseerde tijdelijke serienummers:

SEND ID		
DAY→	KEY→	ID
D01	K-A	ID 01 ID ... ID 72
D...	K-..	ID 01 ID ... ID 72
D14	K-N	ID 01 ID ... ID 72

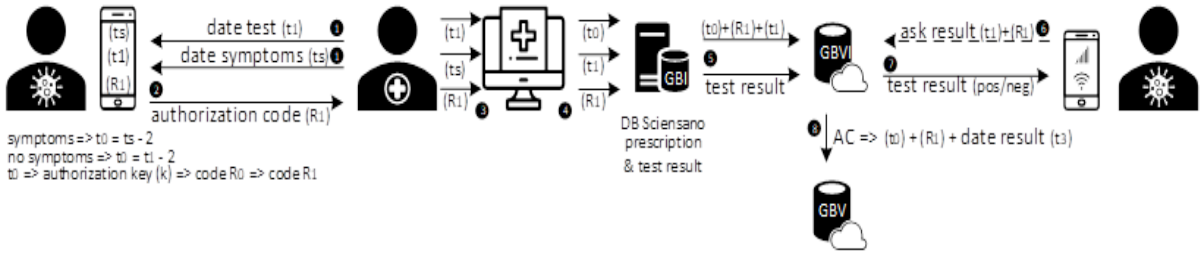
RECEIVED ID		
DAY→	ID	→SIGNAL
D01	ID X ID Y ID ..	-68 -68 -...
D...	ID X ID Y ID ..	-70 -73 -...
D14	ID X ID Y ID ..	-90 -76 -...

De app maakt gebruikt van de module “blootstellingsmeldingen COVID-19” van Google en Apple. Meer informatie over deze module van Google en Apple:
Google: https://www.google.com/covid19/exposurenotifications/
Apple: https://www.apple.com/covid19/contacttracing

De Belgische corona notificatie app is in staat om niet-gepersonaliseerde tijdelijke serienummers (Bluetooth-tokens) uit te zenden naar en op te vangen van corona notificatie app’s van andere landen uit de Europese Economische Ruimte (EER). De voorwaarde is wel dat deze app’s technisch gebruik maken van het DP-3T Protocol (Distributed Privacy-Preserving Proximity Tracking) en de module van Google en Apple.

2.3.2. Gegevensverwerkingen bij afnemen COVID-19 test

Schema van afnemen COVID-19 test tot ontvangen van het testresultaat



Overzicht afkortingen

datums

t0 = vermoedelijke datum van besmetting

- bij symptomen = datum begin symptomen (ts) - 2

- als aymptomatisch = datum test (t1) - 2

t1 = datum wanneer de test werd afgenomen (of de datum van consultatie, waarbij een labo aanvraag werd opgemaakt)

t2 = datum dat het labo het testresultaat overmaakt aan Sciensano

t3 = datum wanneer de app de melding van het testresultaat heeft verwerkt

ts = datum begin symptomen

sleutels

TEK (Temporary Exposure Key) = beveiligde sleutel (wijzigt dagelijks) om willekeurige ID's aan te maken

K = unieke geheime autorisatiesleutel aangemaakt in de app

codes

ID = willekeurige code aangemaakt op basis van de beveiligde sleutel (TEK), ook niet-gepersonaliseerd tijdelijk serienummer genoemd.

R0 = persoonlijk testnummer aangemaakt in de app, op basis van de unieke geheime sleutel (K)

R1 = gedeelde testcode aangemaakt in de app, op basis van het persoonlijk testnummer (R0)

AC = autorisatiecode die bestaat uit een digitale handtekening op de testcode en relevante data.

Gegevensbanken in beheer van Sciensano

GBI (Gegevensbank I) = databank voor het manuele contactonderzoek (met onder andere voorschriften en resultaten van labotesten voor COVID-19). Deze databank levert gegevens aan het platform zonder dat deze daar zelf deel van uitmaakt.

GBV (Gegevensbank V) = databank voor de uitwisseling van de beveiligde sleutels, met als doel andere burgers te waarschuwen dat ze in contact kwamen met een besmette persoon.

GBVI (Gegevensbank VI) = databank voor de uitwisseling van de beoordeling van het testresultaat, ook Gegevensbank IV genoemd, met als doel de besmette persoon op de hoogte te brengen en het aanmaken van een autorisatiecode (AC) en doorsturen naar Gegevensbank V.

Informeren van de burger over de mogelijkheden van de app

De burger laat een COVID-19 test afnemen bij een zorgverlener. De arts die een opsporingstest voor COVID-19 voorschrijft, vraagt aan de burger of deze de contactopsporingsapplicatie gebruikt. Als de burger de app heeft, licht de arts beknopt toe dat er een mogelijkheid is om een melding van het testresultaat te ontvangen in de app. En dat bij een eventueel positief testresultaat de burger een vrije keuze heeft om anoniem burgers waarmee hij in contact kwam te waarschuwen via de app. Om het informatieproces te ondersteunen worden er vormingen voor artsen(organisaties) georganiseerd, informatiebrochures verspreid alsook een website (www.coronalert.be) gelanceerd. Ook de schermen van de app, die getoetst werden inzake gebruiksvriendelijkheid, bevatten de nodige toelichtingen.

Aanmaken van de gedeelde testcode

Indien de burger de app hiervoor wil gebruiken, dan gaat de arts na of er symptomen zijn. Bij symptomen bepaalt de arts in samenspraak met zijn patiënt welke de datum is van de start van de symptomen (ts). Bij afwezigheid van symptomen wordt deze datum niet bepaald. De arts vraagt aan de burger om de datum afname test (t1) in de app in te geven, en bij symptomen bijkomende de startdatum (ts) ervan in te voeren. In de achtergrond bepaalt de app vermoedelijke datum van besmetting (t0). Bij symptomen is deze datum, datum beginsymptomen (ts) verminderd met 2 dagen. Bij afwezigheid van symptomen is deze datum, datum van de test (t1) verminderd met 2 dagen. Daarna maakt de app een unieke geheime autorisatiesleutel (K) aan, en daarna op basis van die sleutel een persoonlijk testnummer (R0). Daarna maakt de app een gedeelde testcode (R1) aan, en maakt

deze zichtbaar in de app. De burger deelt deze code met de arts. Dit kan via een gesprek, aflezen van het scherm of inscannen van de code door de arts.

Communiceren van testcode naar Sciensano

De arts registreert de testcode (R1), de datum van de afname test (of consultatie) (t1) en bij symptomen de startdatum (ts) in een eForm (eFormulier). De vermoedelijk datum besmetting (t0) wordt net zoals in app berekend op basis van de ingevoerde informatie. Dit formulier wordt verstuurd naar Sciensano. Standaard is dit eFormulier "Melding en labo-aanvraag bij vermoeden van besmetting SARS-CoV-2". Sciensano verwerkt en bewaart de informatie in de reeds bestaande gegevensbank voor de voorschriften en testresultaten (DB Sciensano prescription & test result).De arts heeft ook de mogelijkheid om te verklaren dat er een COVID-19 besmetting is, zonder hiervoor het testresultaat af te wachten. De arts registreert in dit geval de testcode (R1), de vermoedelijk datum besmetting (t0) en datum van de afname test (of consultatie) (t1) in het eFormulier "Directe aanvraag contactopvolging bij zeer sterk vermoeden van besmetting COVID-19, onafhankelijk van het testresultaat". Dit kan in combinatie met het eFormulier "Melding en labo-aanvraag bij vermoeden van besmetting SARS-CoV-2".

Wat als een burger een test laat afnemen zonder een consultatie bij een arts? Via afzonderlijke website zullen burgers, in bezit van een Corona Testvoorschriftcode oftewel CTPC code (bv. na terugkeer uit een rode zone), een test kunnen registeren en ook de datum afname test (t1) en/of datum start symptomen (ts), gevolgd door de testcode (R1). Zie webformulier op https://coronalert.be/nl/coronalert-formulier/

Indien er voor een labotestvoorschrift geen testcode (R1) wordt teruggevonden binnen Gegevensbank I dan zal de burger voor wie er een test werd voorgeschreven een SMS ontvangen;Deze SMS zal verstuurd worden vanuit Gegevensbank I van Sciensano waarin zich in het kader van manuele contact tracing GSM-nummers bevinden. Deze SMS[8] bevat de CTPC activatiecode van de test en de link naar het webformulier. Door te klikken op de URL in deze SMS wordt de app geactiveerd en wordt de testcode vanuit de app naar het mobiele webformulier gestuurd. De gebruiker wordt vervolgens gevraagd om zijn/haar INSZ-nummer in te voeren en vervolgens worden de vermelde gegevens naar Gegevensbank I van Sciensano gestuurd.Opgelet: het INSZ-nummer dat nodig is voor koppeling in Gegevensbank I wordt niet in de app maar enkel in het webformulier ingevoerd en enkel verwerkt op de systemen die instaan voor het ondersteunen van het labotest-proces.

Uitvoeren proces PCR test COVID-19

Het proces van de PCR test geeft aanleiding tot het bekomen van een positief of negatief testresultaat. Dit proces bestaat uit het nemen van een staal voor PCR (huisarts/triagepost/ziekenhuis), opsturen naar een labo, verwerking test in een labo, testresultaat delen met Sciensano en de huisarts.

Verwerken van het testresultaat bij Sciensano

Zodra Sciensano een testresultaat ontvangt van een labo, start een proces van verwerking om het manuele contactonderzoek te ondersteunen en daarnaast ook de app. Voor de app start een proces van verwerking waarbij Sciensano de beoordeling van het testresultaat (positief/negatief) kopieert

[8] Dit SMS systeem werd op basis van ervaringen na de lancering van de app bijkomend ontwikkeld omdat het registreren van de testcode door zorgverleners, die tijdens deze gezondheidscrisis reeds een hoge werklast hebben, moeilijkheden vertoonde.

naar gegevensbank VI. Na deze actie verwijdert Sciensano de gedeelde testcode (R1) in zijn gegevensbank (GBI). De burger wordt geïdentificeerd op basis van de gedeelde testcode (R1) en de vermoedelijke datum besmetting (t0).

Opvragen van het testresultaat in de app

Om de 2 uur stelt de app, in de achtergrond en op automatische wijze, een vraag aan gegevensbank VI van Sciensano om het testresultaat te vernemen. Om meldingen van testresultaten aan foute personen te vermijden stuurt de app de gedeelde testcode (R1) en de de datum afname test (t1) mee in de vraag. In technische taal noemt men dit gehele proces “polling” en in het schema is dit beschreven als “ask result (t0) + (R1)”.

De gegevensbank VI beschikt over drie mogelijke antwoorden op de vraag van de app:

- er is nog geen testresultaat beschikbaar
- er is een testresultaat beschikbaar, en deze werd beoordeeld als negatief
- er is een testresultaat beschikbaar, en deze werd beoordeeld als positief

Bij een negatief testresultaat heeft de huisarts de mogelijkheid om dit te laten ‘overschrijven’ als een positief testresultaat. De arts registreert dit via het eFormulier “Aanvraag contactopvolging bij negatief testresultaat”. Dit proces van overschrijven van een negatief testresultaat staat beschreven op volgende website https://covid19lab.healthdata.be/data-collection/resultflagssuspicionfalsenegativetest

Het technologisch kader van de app heeft geen rechtstreekse mogelijkheid om een negatief testresultaat te laten wijzigen naar een positief testresultaat. De voorziene werkwijze is dat de arts vraagt aan de besmette persoon om opnieuw een gedeelde testcode aan te maken, en door te geven. De arts vult het eFormulier “Directe aanvraag contactopvolging bij zeer sterk vermoeden van besmetting COVID-19, onafhankelijk van het testresultaat” in, en stuurt deze door naar Sciensano. Na een aantal uren zal de besmette persoon een nieuwe melding ontvangen, ditmaal met de boodschap dat er een positief testresultaat is. Als de arts die werkwijze niet toepast, dan is blijft het manuele contactonderzoek van toepassing en heeft de besmette persoon geen mogelijkheid om via de app andere burgers te waarschuwen.

2.3.3. Verwerkingen na ontvangen melding testresultaat

Wanneer de burger in de app een melding ontvangt met de beoordeling van het testresultaat, dan kan hij via de app de burgers die met hem in contact kwamen waarschuwen. Deze mogelijkheid is actief in de app gedurende een periode van 24 uur. Nadien wordt deze optie uitgeschakeld en de acties uitgevoerd die horen bij “niet waarschuwen van burgers via de app”.

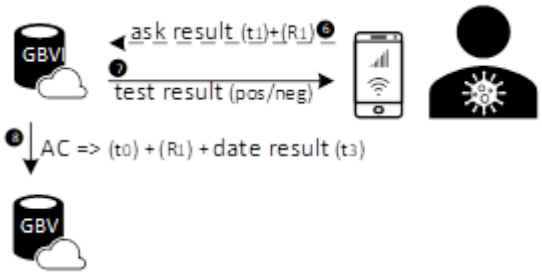
De waarschuwing gaat naar burgers die de Belgische corona notificatie app gebruiken, of een corona notificatie app aangeboden in een ander land van de Europese Economische Ruimte (EER). De voorwaarde is wel dat deze app technisch gebruik maakt van het DP-3T Protocol (Distributed Privacy-Preserving Proximity Tracking).

Doorsturen van een handtekening van gegevensbank VI naar gegevenbank V

Zodra de app de melding ontvangt, dan registreert gegevensbank VI de datum (t3) van deze actie[9]. Bij een positieve beoordeling vermeld in hettestresultaat, brengt gegevensbank VI (DB2) de gegevensbank V (DB1) van Sciensano op de hoogte. Hiervoor maakt gegevensbank VI een unieke handtekening aan, die bestaat uit de gedeelde testcode (R1) van de burger, de vermoedelijke datum besmetting (t0) en datum dat het testresultaat werd opgevraagd door de app (t3).

Nadat de gegevensbank VIde handtekening heeft aangemaakt en doorgestuurd, verwijdert Sciensano de vermoedelijke datum van besmetting (t0), de gedeelde testcode (R1) en het testresultaat uit gegevensbank VI (DB2 in het schema).

Schema doorsturen handtekening van gegevensbank VI naar gegevenbank V



Niet waarschuwen van burgers via de app
Als de burger aangeeft burgers niet te willen waarschuwen, dan verwijdert de app de volgende informatie:

- de vermoedelijke datum besmetting (t0)
- persoonlijk testnummer (R0)
- de gedeelde testcode (R1)
- de datum wanneer de test werd afgenomen (t1)
- unieke geheime autorisatiesleutel (K) (die werd gebruikt om het persoonlijk testnummer (R0) aan te maken)
- de datum wanneer de app de melding heeft ontvangen (t3)

Waarschuwen van burgers via de app
Als de burger aangeeft burgers te willen waarschuwen, dan vraagt de app eerst in welke landen hij was in periode van datum vermoeden besmetting tot ontvangen van de melding. Daarna deelt de app de volgende informatie met gegevensbank V van Sciensano:

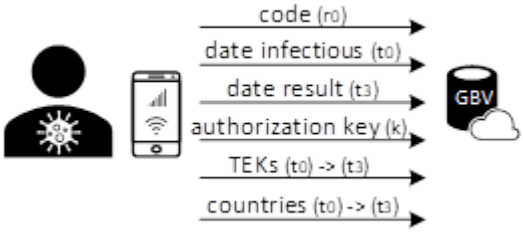
- de vermoedelijke datum besmetting (t0)
- persoonlijk testnummer (R0)
- unieke geheime autorisatiesleutel (K) (die werd gebruikt om het persoonlijk testnummer (R0) aan te maken)
- de datum wanneer de app de melding heeft ontvangen (t3)

[9] Deze actie gebeurt 1 keer per uur.

- de beveiligde sleutels (TEKs) van de dagen tussen vermoedelijke datum besmetting (t0) en de datum wanneer de app de melding heeft ontvangen (t3)
- overzicht van landen in de aangegeven periode

Na het doorsturen van de laatste beveiligde sleutel (TEK), verwijdert de app de vermoedelijke datum besmetting (t0), het persoonlijk testnummer (R0), de gedeelde testcode (R1), de datum wanneer de test werd afgenomen (t1) de unieke geheime autorisatiesleutel (K) en de datum wanneer de app de melding heeft ontvangen (t3).

Schema van het doorsturen van informatie naar gegevensbank V van Sciensano om andere burgers te waarschuwen



Verwerken van de vraag om te waarschuwen (Sciensano)

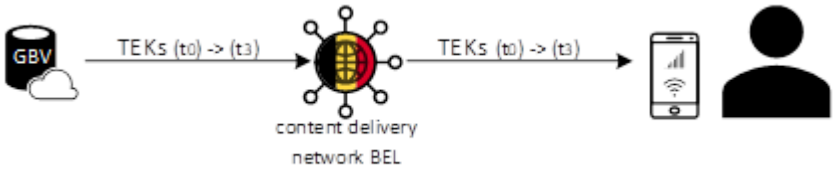
Gegevensbank V van Sciensano verwerkt om de 2 uur alle ontvangen informatie, en voert een autorisatiecontrole uit. Enkel burgers met een positieve beoordeling van het testresultaat mogen burgers waarschuwen. Deze controle bestaat uit volgende stappen:

- berekenen van gedeelde testcode (R1), aan de hand van de vermoedelijke datum besmetting (t0), de unieke geheime autorisatiesleutel (K) en het persoonlijk testnummer (R0)
- maken van de unieke handtekening (AC), die bestaat uit gedeelde testcode (R1), de vermoedelijke datum besmetting (t0), en de datum wanneer de app de melding heeft ontvangen (t3)
- nagaan of er handtekening (AC) bestaat in de lijst (van de afgelopen 48 uur) die gegevensbank VI (DB2 in het schema) heeft doorgestuurd

Waarschuwen van burgers die een corona notificatie app gebruiken

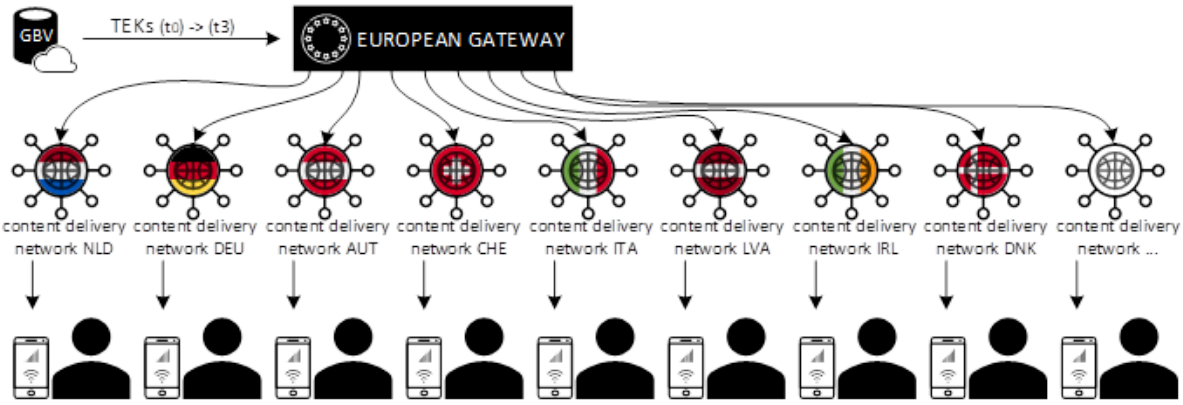
Indien er een autorisatiecode (AC) bestaat, dan stuurt de Gegevensbank V van Sciensano de beveiligde sleutels (TEK keys) van de dagen tussen vermoedelijke datum besmetting (t0) en de datum wanneer de app de melding heeft ontvangen (t3) naar het content delivery network (CDN). Dit technisch onderdeel zorgt ervoor dat alle burgers, die de Belgische corona notificatie app gebruiken, deze sleutels ontvangen. De app zal daarna een onderzoek uitvoeren, om na te gaan of de app beschikt over ontvangen willekeurige ID's die werden aangemaakt met die sleutels. Indien er een overeenkomst is, gaat de app na hoe lang het contact was en wat de onderlinge afstand was tussen de gebruiker en een besmettelijke persoon. (Het toegepaste algoritme hiervoor is gedocumenteerd in hoofdstuk 5.3 van https://www.esat.kuleuven.be/cosic/sites/corona-app/wp-content/uploads/sites/8/2020/08/coronalert_belgium_description_v1_2.pdf). In functie daarvan zal de app een waarschuwing geven aan de burger, en hem adviseren wat te doen.

Schema waarschuwen burgers in België



Als de burger heeft aangeven in andere Europese land te hebben verbleven, dan zal gegevensbank V van Sciensano de beveiligde sleutels (TEKs) van de dagen tussen vermoedelijke datum besmetting (t0) en de datum wanneer de app de melding heeft ontvangen (t3) delen met een Europese gatewaydienst[10] van de Europese Commissie. Deze gateway zal de informatie delen met het content delivery network van de opgegeven landen, om op die manier de burgers te waarschuwen. Elke corona notificatie app zal ministens 1 keer per dag de sleutels ophalen via het content delivery network.

Schema waarschuwen burgers in andere Europese landen



De interoperabiliteitsdienst (gateway) is een digitale infrastructuur die zorgt voor de veilige overdracht van gegenereerde sleutels tussen de backend servers van de deelnemende nationale contacttraceer- en waarschuwingsapplicaties. Daarbij deelt de gateway de minimale informatie die nodig is om een persoon te waarschuwen als deze is blootgesteld aan een geïnfecteerde persoon die ook gebruik maakt van een van de deelnemende apps.

De uitgewisselde gegevens worden slechts gedurende een periode van maximaal 14 dagen in de gateway opgeslagen. Geen andere informatie dan de sleutels, gegenereerd door de nationale apps, zal door de Gateway worden behandeld.

Het ontwerp van de gateway is gebaseerd op de richtsnoeren voor interoperabiliteit, de reeks technische specificaties die tussen de lidstaten en de Commissie zijn overeengekomen, de beginselen van de EU-toolbox en de richtsnoeren van de Commissie en het Europees Comité voor gegevensbescherming inzake gegevensbescherming voor het traceren van contacten en het waarschuwen van apps. (Voor meer informatie zie: https://ec.europa.eu/commission/presscorner/detail/nl/QANDA_20_1905).

[10] https://ec.europa.eu/commission/presscorner/detail/nl/ip_20_1043

De gateway is ontwikkeld en opgezet door de bedrijven T-Systems en SAP, en wordt geëxploiteerd vanuit het datacenter van de Commissie in Luxemburg.

2.3.4. Nieuw (update Coronalert): andere app-gebruikers waarschuwen via een 12-digit covicode

Vanaf de tweede helft van 2021 zal wordt er een derde methode om een positief testresultaat aan de app te koppelen geïntroduceerd: een burger met een positieve test neemt contact op met het callcenter en ontvangt een 12-cijferige covicode (deze code kan via de telefoon worden afgelezen of per sms worden verzonden) die autorisatie geeft voor het opladen van de sleutels. Een voorbeeld van een covicode staat hieronder:

4287-6231-7759.

De burger voert vervolgens deze covicode in Coronalert in samen met de datum ts van het begin van de symptomen (als er geen symptomen zijn wordt de datum t0 waarop de test werd afgenomen ingevoerd); deze data kunnen maximaal 12 dagen in het verleden liggen (afgedwongen door de app). Vervolgens wordt de gebruiker gevraagd om de TEK-sleutels op te laden van de besmettelijke periode die naar schatting twee dagen voor het begin van de symptomen begint (of, als er geen symptomen zijn, twee dagen voor de testdatum).

Deze aanpak heeft het voordeel dat hij begrijpelijk is voor de burger, aangezien hij alleen wordt uitgevoerd wanneer er een positieve test is. Bovendien biedt deze aanpak ook oplossingen voor rapid tests of zelftests. Een ander voordeel is dat de burger begeleiding kan krijgen van het callcenter.

Om misbruik van covicodes te voorkomen, kunnen deze codes slechts één keer worden gebruikt. Bovendien zijn ze slechts een beperkte tijd geldig (24 minuten georganiseerd in intervallen van 5 minuten - dit is inclusief een marge van 2 minuten ervoor en erna om rekening te houden met de scheefheid van de klok). Indien een code bijvoorbeeld wordt uitgegeven tussen 16:50 en 16:54, is hij geldig tussen 16:48 en 17:12 en indien een code wordt uitgegeven tussen 00:00 en 00:04, is hij geldig tussen 23:58 (vorige dag) en 00:22.

Om een complexe live interactie tussen het systeem van het callcenter en de backend van de app te vermijden, worden codes vooraf per batch gegenereerd, waarbij een batch overeenkomt met een dag. Deze batches worden op een veilige manier off-line overgebracht naar het callcenter.

In het callcenter leest een eenvoudige (web)applicatie de volgende ongebruikte code uit het bestand met covicodes door de juiste dag, de juiste periode van 5 minuten uit de batch en de volgende ongebruikte code in de batch te selecteren. In de backend is een soortgelijke lijst aanwezig om de geldigheid te verifiëren.

2.4. Verwerkingsdoeleinden

Zoals bepaald in art. 14 § 4 van het KB nr. 44 en het Samenwerkingsakkoord:

- De digitale contactopsporingsapplicatie ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking heeft als doel de gebruikers te informeren dat zij een risicovol contact hebben gehad met een andere besmette

gebruiker, zonder dat de besmette gebruiker door de digitale contactopsporingsapplicatie wordt geïdentificeerd, en met als verder doel dat de verwittigde gebruiker dan zelf vrijwillig de nodige stappen zou ondernemen, op basis van de aanbevelingen van Sciensano en de bevoegde gefedereerde entiteiten, om verdere verspreiding van het coronavirus COVID-19 te voorkomen.

2.5. Belangen bij de gegevensverwerkingen

De belangen van de betrokken overheden situeren zich op volgende vlakken

- vertrouwen door de burger dat de gegevensverwerkingen een waardevol doel nastreven
- het aanbieden van een kwaliteitsvol product dat de gegevensverwerkingen bewerkstelligt
- een gunstige medische context voor de nagestreefde doeleinden van de gegevens-verwerkingen

Vertrouwen bij het brede publiek

De waarde van de app moet correct gepositioneerd worden: het gebruik van de app helpt in eerste instantie de hele maatschappij sneller uit de lockdown te komen (of een nieuwe lockdown te vermijden) en helpt de gebruiker zelf maar in tweede orde. (Het laat hem toe om een besmettingsrisico sneller vast te stellen). Het gebruik is een teken van burgerzin en solidariteit: als je besmet raakt laat het toe om de mensen waarmee je in contact bent geweest te waarschuwen en de verdere verspreiding van het virus tegen te gaan.

Kwaliteitseisen

De app moet voldoen aan hoge kwaliteitseisen: eenvoudig te installeren en gebruiken, beperkt batterijverbruik om gegevensverwerkingen mogelijk te maken. Inzake gebruiksvriendelijkheid werden er ‘usability & experience’ testen uitgevoerd.

De serverinfrastructuur moet voldoen aan hoge kwaliteitseisen: goede performantie, bestand tegen aanvallen. De infrastructuur moet zo snel mogelijk interoperabel gemaakt worden met de infrastructuur in het buitenland.

Het belang van kwaliteit geldt ook ten aanzien van de reputatie van de onderaannemers van de betrokken overheden.

Medisch

De effectiviteit van het gezondheidsadvies: duidelijke communicatie over implicaties van risico’s en wat de burger moet doen *(contacteren huisarts, test, quarantaine).*

Het aantal nieuwe besmettingen per dag mag niet te hoog liggen.

Er moeten voldoende testen beschikbaar zijn en de testresultaten moeten zo snel mogelijk beschikbaar zijn (idealiter <48u).

De data van de labo’s en huisartsen dient betrouwbaar te zijn.

2.6. Verwerkingslocaties

De gegevens met betrekking tot de digitale contactopsporing worden verwerkt binnen de EU.

Er vinden enerzijds verwerkingen op het toestel van de gebruiker plaats en anderzijds binnen de serverinfrastructuur. (Zie tabel pagina 8).

De serverinfrastructuur van de nationale app bevindt zich in Duitsland.

Zoals aangegeven in hoofdstuk 2.2 kan bij het gebruik van een service-laag van het besturingssysteem de dienstenaanbieder extra verwerkingen voorzien voor telemetrie. Afhankelijk van de voorwaarden van Google of Apple kan de verwerking van deze gegevens buiten Europa gebeuren. Het valt op te merken dat de verzamelde gegevens geen inhoudelijke gegevens van app bevatten en dat deze verwerkingen gebeuren met instemming van de eigenaar van de smartphone.

2.7. Technieken en methoden van de gegevensverwerkingen

De toepassing van de gegevensbescherming door ontwerp en door standaardinstellingen, principes van de Algemene Verordening Gegevensbescherming, stond centraal bij de ontwikkeling van een digitale contactopsporingsapplicatie. Het Europees Comité voor gegevensbescherming beveelt op dit vlak digitale contactopsporingsapplicaties aan die gebruik maken van Bluetooth en die gedecentraliseerd werken.

DP-3T[11] is een samenwerkingsverband van onderzoekers uit heel Europa die hun krachten hebben gebundeld om een open technische oplossing voor contactopsporing te creëren voor de COVID-19-epidemie die de privacy respecteert. De DP-3T oplossing voldoet aan de hogervermelde vereisten.

De meest recente open source implementatie steunt op de Google/Apple API[12]. De specifieke integratie met de gezondheidsinfrastructuur moet voor elk land afzonderlijk ontwikkeld worden; hiervoor zijn ook modellen voorzien.

De DP-3T oplossing is gedecentraliseerd, wat betekent dat informatie over contacten lokaal op de smartphone bewaard blijven en de beslissing of de burger een risico loopt op de smartphone zelf genomen wordt. Er is een centraal register dat enkel willekeurige sleutels en een geldigheidsperiode bevat. Het gebruik van een gedecentraliseerde architectuur is een noodzakelijke voorwaarde om toegang te krijgen tot de Google/Apple API.

2.8. 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

- *Aanbeveling (EU) 2020/518 van de Commissie van 8 april 2020 over een gemeenschappelijke toolbox voor het gebruik van technologie en gegevens om de Covid- 19-crisis te bestrijden en*

[11] https://github.com/DP-3T/documents
[12] Application Programming Interface: definieert de interacties tussen meerdere software componenten.

te boven te komen, met name wat mobiele applicaties en het gebruik van geanonimiseerde mobiliteitsgegevens betreft

- *Guidelines 04/2020 from the European Data Protection Board on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. Adopted on 21 April 2020*
- *Mededeling van de Commissie: Richtsnoeren in verband met gegevensbescherming voor apps ter ondersteuning van de bestrijding van de COVID-19-pandemie (2020/C 124 I/01)*
- *Uitvoeringsbesluit (EU) 2020/1023 van de Commissie van 15 juli 2020 tot wijziging van Uitvoeringsbesluit (EU) 2019/1765 wat betreft de grensoverschrijdende uitwisseling van gegevens tussen nationale mobiele applicaties voor het traceren en waarschuwen van contacten met het oog op de bestrijding van de COVID-19-pandemie*

Federaal en interfederaal

- *Koninklijk besluit nr. 44 van 26 juni 2020 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden 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*
- *Koninklijk besluit van 17 september 2020 tot uitvoering van het koninklijk besluit nr. 44 van 26 juni 2020 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden 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*
- *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*
- *Uitvoerend samenwerkingsakkoord van 13 oktober 2020 tussen de Federale staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie, betreffende de digitale contactopsporingsapplicatie(s), overeenkomstig artikel 92bis, §1, derde lid, van de Bijzondere wet van 8 augustus 1980 tot hervorming der instellingen*
- *Wet van 9 oktober 2020 houdende instemming met 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 COVID19 besmet zijn op basis van een gegevensbank bij Sciensano*
- *Wet van 25 februari 2018 tot oprichting van Sciensano*
- *Adviezen en werkzaamheden van de Werkgroep voor de ontwikkeling van een Exit Strategy (GEES) en het Interfederaal Comité Tracing en Testing Covid-19*

Hierbij is het belangrijk om op te merken dat het Samenwerkingsakkoord van 25 augustus 2020 voorwerp uitmaakt van een annulatieberoep bij de Raad van State. De uitkomsten van het annulatieberoep zullen, van zodra gekend, verwerkt worden in een update van deze GEB.

Deelstatelijk:

- *Decreet van 21 november 2003 betreffende het preventieve gezondheidsbeleid (voor Vlaanderen)*
- *Decreet van 2 mei 2019 tot wijziging van het Waalse Wetboek van Sociale Actie en Gezondheid wat betreft de preventie en de bevordering van de gezondheid (voor Wallonië)*
- *Ordonnantie van 19 juli 2007 betreffende het preventieve gezondheidsbeleid en het besluit van 23 april 2009 van het Verenigd College van de Gemeenschappelijke Gemeenschapscommissie betreffende de profylaxe tegen overdraagbare ziekten (voor Brussel)*
- *Decreet van het Parlement van de Duitstalige Gemeenschap van 1 juni 2004 betreffende de gezondheidspromotie en inzake medische preventie en zijn uitvoeringsbesluiten*
- *Decreet van 2 oktober 2020 houdende instemming met 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 COVID19 besmet zijn op basis van een gegevensbank bij Sciensano*
- *Decreet van 12 oktober 2020 houdende instemming met 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 COVID19 besmet zijn op basis van een gegevensbank bij Sciensano*
- *Decreet van 30 september 2020 houdende instemming met 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, gezondheidsinspectiediensten en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID19 besmet zijn op grond van een gegevensbank bij Sciensano*
- *Ordonnantie van 1 oktober 2020 houdende instemming met 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, gezondheidsinspectiediensten en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID19 besmet zijn op grond van een gegevensbank bij Sciensano*

2.9. Bewaartermijnen

De maximale bewaartermijnen zijn wettelijk bepaald.

- Het testresultaat wordt ten laatste vierentwintig uur na het tonen van het resultaat aan de gebruiker uit de app verwijderd.
- Alle gegevens met betrekking tot contacten tussen gebruikers, opgeslagen op het toestel van de gebruiker, worden gewist ten laatste drie weken nadat ze zijn gegenereerd op het toestel van de gebruiker van een digitale contactopsporingsapplicatie. Teneinde het zelfbeschikkingsrecht van de gebruiker maximaal te kunnen garanderen, gebeurt de deactivatie van de digitale contactopsporingsapplicatie op het toestel van de gebruiker door de gebruiker zelf.
- Gegevens die terechtkomen in de gegevensbank met de loglijst mogen niet meer gebruikt worden door de mobiele applicatie van de digitale contactopsporingsapplicatie op het toestel van de gebruiker. De in deze gegevensbank bewaarde informatie dient te worden gewist ten laatste drie weken nadat ze in deze gegevensbank werd opgenomen. Gelet op de incubatietijd van het coronavirus COVID-19, is een termijn van drie weken opportuun. Deze gegevensbank wordt ten laatste gedeactiveerd eenentwintig dagen na de publicatie van het koninklijk besluit dat het einde van de toestand van de coronavirus COVID-19-epidemie afkondigt.

Zoals uit de beschrijving van de gegevensstromen en het Uitvoerend Samenwerkingsakkoord blijkt, blijven de gepseudonimiseerde gegevens voor meldingen aan nabije contacten slechts 14 dagen bewaard in plaats van de voorziene maximumtermijn van drie weken in het Samenwerkingsakkoord. Gegevens in de testresultaten-gegevensbank (Gegevensbank VI) en bepaalde gegevens in de gegevensbank voor manuele contact tracing (GBI) zullen tevens direct verwijderd worden na bepaalde acties. Zie beschrijving van de gegevensstroom in punt 2.3.:

- Nadat dat de beoordeling van het testresultaat (positief/negatief) gekopieerd werd naar de testresultaten-gegevensbank verwijdert Sciensano de gedeelde testcode (R1) in zijn gegevensbank manuele contact tracing (GBI).
- Nadat de app de gegevens heeft gedownload en Gegevensbank VI de autorisatiecode heeft aangemaakt, verwijdert Sciensano de vermoedelijke datum van besmetting (t0), de gedeelde testcode (R1) en het testresultaat uit de testresultaten-gegevensbank. Hetzelfde gebeurt wanneer een burger met een positief testresultaat aangeeft niet te willen waarschuwen. Als het resultaat van een test veertien dagen na de opslag ervan in Gegevensbank VI niet gedownload is, worden het resultaat van de test en de bijhorende testcodes en data verwijderd uit Gegevensbank VI

Sectie III: Consultatieproces

In de Kamercommissie Economie vond er op 28 april 2020 hoorzittingen plaats met experten van de academische sector, het middenveld en de overheid op vlak van ICT, privacy, mensenrechten en (cyber)security.[13] Het parlementaire debat leidde tot een wetsvoorstel waarover een advies werd gevraagd aan de Gegevensbeschermingsautoriteit

[13] https://www.lachambre.be/FLWB/PDF/55/1182/55K1182005.pdf

- Advies nr. 43/2020 van 26 mei 2020 betreffende een wetsvoorstel betreffende het gebruik van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking *(CO-A-2020-049)*

Verdere uitwerking van de vereisten *(o.a. juridisch, technisch, epidemiologisch)* van de opsporingsapplicatie vonden plaats binnen de schoot van de Interfederale Werkgroep Testing en Tracing. Deze werkgroep bestaat uit vertegenwoordigers van de federale en deelstatelijke (gezondheids)administraties alsook deskundigen inzake informatica en infectieziekten. Bij de verdere uitwerking werden inzichten van het consultatieproces in rekening gebracht. *(Zie bijvoorbeeld verwijzingen naar het GBA-advies in het wettelijk kader van de contactopsporingsapplicatie).*

De Interfederale Werkgroep vond het tevens belangrijk om een openbare raadpleging te organiseren waarbij onder andere aandacht wordt besteed aan volgende vraagstukken:

- Op welke leeftijd moeten minderjarigen zelfstandig kunnen beslissen over het gebruik van de app?
- Hoe kunnen we ervoor zorgen dat de app inclusief is en zoveel mogelijk mensen in de samenleving bereikt?
- Hoe kunnen we het vertrouwen en het begrip van de bevolking in de app vergroten?
- Is de privacyverklaring duidelijk en voldoende?
- Hoe kan de gebruiksvriendelijkheid van de app worden vergroot?
- Hoe kunnen medische professionals een rol spelen bij het stimuleren van het gebruik van de app?
- Wie moet worden opgenomen in een onafhankelijke toezichtscommissie?

De openbare raadpleging heeft tot doel om vanuit het grote publiek en de relevante stakeholders de belangrijkste juridische, ethische, sociale, technische en veiligheidsuitdagingen te identificeren die verband houden met de ontplooiing van een Bluetooth-contactopsporingsapplicatie in België: zie https://www.esat.kuleuven.be/cosic/sites/corona-app/nl/ . Ze is gericht op

- Academische experts in rechten, sociale wetenschappen, techniek, informatica, geneeskunde, …
- Niet-academische deskundigen en professionals op het gebied van app-development, cybersecurity, privacy en gegevensbescherming, volksgezondheid, geneeskunde, e-inclusion
- Maatschappelijk middenveld
- Gemeenten
- Bezorgde burgers

De raadpleging wordt gecoördineerd door de COSIC-onderzoeksgroep (KU Leuven) en liep van5 augustus 2020 tot en met 31 augustus 2020. Het rapportvan deze consultatie is publiek beschikbaar. Dit rapport geeft ook weer op welke manier er rekening werd gehouden met de uitkomsten van de consultatie.

Sectie IV: Beoordeling noodzakelijkheid & proportionaliteit

4.1. 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). De verwerkingsactiviteiten hebben namelijk als oogmerk om de verspreiding van COVID-19 in te dijken en de bevolking tegen deze epidemie te beschermen.De app is geregeld via het volgende wettelijke kader::

- Voorheen (tijdelijk): *Koninklijk besluit nr. 44 van 26 juni 2020 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden 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*
- Heden en retroactief van toepassing: *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*

Het Samenwerkingsakkoord en het Uitvoerend Samenwerkingsakkoord voorzien dat Sciensano de verwerkingsverantwoordelijke is voor de gegevensbank met de centrale loglijst van de opsporingsapplicatie (GBV) en de gegevensbank met de tijdelijke bewaring van testresultaten (GBVI). Het wettelijk kader hieromtrent is noodzakelijk en garandeert de vrije keuze van de burger om een digitale contactopsporingsapplicatie te installeren, te gebruiken en te de-installeren en de vrije keuze om zijn gegevens naar het centrale platform door te sturen..

4.2. 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).

Los van deze uitzondering op het verbod inzake de verwerking van persoonsgegevens, blijft het van belang om de vrije keuze van de burger, om al dan niet (gezondheids)gegevens via de app of bijhorende serverinfrastructuur te verwerken, te benadrukken. Een gebruiker van de contactopsporingsapplicatie heeft de mogelijk om wel of niet in te stemmen met het opvragen van een testresultaat en het opladen van de noodzakelijke gegevens (zoals vermoedelijke datum van besmetting) indien hij contacten wil waarschuwen.

4.3. Doelbinding

De toelichting van het juridisch kader van de contactopsporingsapplicatie geeft op duidelijke wijze de grenzen inzake het gebruik van de contactopsporingsapplicatie en zijn gerelateerde gegevensverwerking aan. Het enige doel is om burgers op vrijwillige basis te waarschuwen voor mogelijke blootstelling aan het virus. Deze opdrachten zijn omschreven in de respectievelijke KB's en samenwerkingsovereenkomsten.

De verwerkingen door het platform beperken zich tot de verwerkingen zoals omschreven in hoofdstuk 2.3 van deze GEB.

De gegevens worden enkel verder verwerkt zoals omschreven in 2.3 indien de betrokkene daarmee instemt Deze gegevens worden niet verrijkt of verwerkt met gegevens uit andere bronnen, met

uitzondering van de testresultaten. Voor het verwerken van deze testresultaten heeft de gebruiker ook zijn instemming gegeven.

Er worden geen andere verwerkingen verricht met de verkregen persoonsgegevens.

4.4. Noodzaak en evenredigheid

De Coronalert App functioneert zonder directe identificatie van personen. Er wordt alleen relevante en absoluut noodzakelijke informatie verzameld.

- Niet-gepersonaliseerde tijdelijke serienummers (via Bluetooth tokens): noodzakelijk om gebruikers van de app op anonieme wijze te waarschuwen dat ze in nabij contact kwamen met een besmet persoon.
- Resultaat labotest: noodzakelijk om acties inzake het waarschuwen van contacten over besmettingsrisico's al dan niet te initiëren
- Vermoedelijke datum besmetting: noodzakelijk om vanuit medisch oogpunt in te schatten voor welke contacten er besmettingsrisico's zijn
- Testcodes: noodzakelijk om te vermijden dat er valse (kwaadwillige) meldingen inzake besmettingsrisico's verstuurd worden
- Verblijf in Europese landen: noodzakelijk om personen waarmee de besmette persoon buiten België in contact kwam te notifiëren

De Coronalert App verwerkt geen locatiegegevens van individuele gebruikers. Voor het meten van nabijheid tussen personen is het immers niet noodzakelijk om hun locatie te kennen. Het systeem slaat ook geen IP-adressen van gebruikers op.

Om de risico's voor de betrokkenen tot een minimum te beperken, mogen de in de centrale databank opgeslagen gegevens niet met andere databanken worden vergeleken.

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").

Sciensano zal alleen kunnen reageren op verzoeken van gebruikers wanneer het mogelijk is om de gegevens die worden verwerkt in het kader van de contactopsporingsapplicatie te koppelen aan de specifieke gebruiker. Om de gegevens aan de gebruiker te kunnen koppelen, zou Sciensano extra gegevens moeten verkrijgen. Aangezien de contactopsporingsapplicatie is gebouwd op technologie die de persoonlijke levenssfeer van de gebruikers zoveel mogelijk moet beschermen, is het niet wenselijk dat Sciensano aanvullende gegevens verwerkt om de gebruiker te identificeren. Op grond van artikel 11 van de AVG kan Sciensano niet worden verplicht om dergelijke aanvullende gegevens te verwerken om de gebruiker te identificeren met als enig doel het naleven van de rechten van de betrokkene op grond van de AVG. Dit betekent dat gebruikers in de praktijk niet in staat zullen zijn om hun rechten als betrokkene uit te oefenen, tenzij er aanvullende informatie aan Sciensano wordt verstrekt. Deze informatie zal worden meegedeeld in de Privacyverklaring ten aanzien van de betrokkenen. Voor gegevensbank V is het tevens zo dat Sciensano de rechtmatigheid van een aanvraag inzake rechten (bv. inzage of verwijdering) niet kan controleren omdat de sleutels niet herleidbaar zijn tot een individu.

Hoewel de uitoefening van de rechten door de hoge mate van pseudonimisatie moeilijk is, wordt het data subject beschermd via korte bewaartermijnen van gegevens (max. 14 dagen) en de ingebedde autonomie voor de gebruiker inzake gegevensverwerkingen. Het downloaden van een testresultaat zorgt er bijvoorbeeld automatisch voor dat gegevens in gegevensbank VI verwijderd worden. De gebruiker kan via de functies van de applicaties tevens zelf beslissen of hij gegevens *(bv. testresultaten, landen van verblijf of sleutels)* wel of niet wil (laten) verwerken.

Sectie V: Informatieveiligheid

5.1. Informatieveiligheid server infrastructuur

Samenvatting

De Coronalert App is ontworpen, gebouwd, gehost en onderhouden met veiligheid als een van de topprioriteiten.

De beslissing om de backend bij AWS te hosten is ook gebaseerd op deze sterke focus op veiligheid. Omdat AWS als een publieke cloud kan worden beschouwd, is het belangrijk om de beveiligingsmaatregelen die worden genomen heel duidelijk en nauwkeurig te formuleren. Deze maatregelen zijn:

1. Het opzetten van de totale architectuur van de applicatie steunt op het principe van security by design. Enkele van de kenmerken van de architectuur van de inzet van de applicatie zijn:
    1. De servers zijn gevestigd in Europa (Frankfurt)
    2. “Data at rest” is geëncrypteerd (AES-256)
    3. “Data in transit” wordt altijd geëncrypteerd (TLS)
2. Het beheer van de informatie en data architectuur gebeurt met een focus op veiligheid en privacy:
    1. Er worden enkel gepseudonimiseerde gegevens bewaard op de back-end systemen.
    2. De 15-cijferige code die toegang geeft tot de resultaten van een test en die de betrokkene toelaat zijn resultaat te bekomen bevat geen gegevens die kunnen teruggebracht worden tot de gebruiker of zijn telefoon.
    3. De 15-cijferige code wordt van de back-end verwijderd zodra de gebruiker het resultaat van zijn test heeft bekomen.
    4. De informatie wordt van de back-end systemen verwijderd wanneer deze niet langer nodig zijn (nadat de resultaten werden bekomen door de gebruiker of ten laatste 14 dagen na de vermoedelijke datum van infectie).
3. Er worden specifieke AWS-tools geïmplementeerd ter ondersteuning van:
    1. Rate limiting
    2. Certificate pinning
    3. Anti DDoS maatregelen
    4. Een reeks veiligheidscontroles om gegevens te beschermen tegen ongeoorloofde toegang, wijziging of verwijdering.

Architectuur

- Het platform wordt geïnstalleerd in 3 AZs (Availability Zones) in eu-central-1 (Frankfurt)
- Alle diensten worden minstens in elke AZ geïnstalleerd.
- S3, CloudFront and ALBs zijn heel schaalbaar

- “Data at rest” is altijd geëncrypteeerd (AES256)
- “Data in transit” is altijd geëncrypteerd (TLS)
- SLA is 99.999%. AWS garandeert 99.9% voor de meeste diensten, maar door de meervoudige uitvoering in 3 AZ’s is de totale beschikbaarheid berekend op 1 - (0.001^3).
- Backups met Point In Time Recovery
- Batches met covicodes worden op een veilige manier off-line naar het callcenter overgebracht (via een SSH-verbinding of een gecodeerde webtransfer).

Data Architectuur

- Enkel gepseudonimiseerde gegevens bewaard in de back-end
- R1 is een 15 cijferige code die een bepaalde test (en het resultaat daarvan) koppelt aan een mobiel apparaat. Het bevat geen informatie over de gebruiker van de telefoon. Het wordt gegenereerd op de telefoon en gecommuniceerd met de arts.
- Deze informatie wordt ook verwijderd van de back-end zodra een testresultaat wordt gedownload.
- Rate limiting, certificate pinning, anti DDoS measures, proof-of-work worden toegepast
- Gegevens worden van de back-end verwijderd wanneer ze niet meer nodig zijn (nadat de resultaten werden gedownload of na t0+14)
- Om misbruik van covicodes te voorkomen, kunnen deze codes slechts eenmaal worden gebruikt. Bovendien zijn ze slechts gedurende een beperkte tijd geldig (24 minuten met intervallen van 5 minuten - dit omvat een marge van 2 minuten voor en na om rekening te houden met de klokvertraging). Indien een code bijvoorbeeld wordt uitgegeven tussen 16:50 en 16:54, is hij geldig tussen 16:48 en 17:12 en indien een code wordt uitgegeven tussen 00:00 en 00:04, is hij geldig tussen 23:58 (vorige dag) en 00:22. Op elk moment zijn er slechts 1000 geldige codes, zodat de kans dat een willekeurige code wordt aanvaard 1 op 1 miljard is. Er is een eenvoudige snelheidsbegrenzer nodig om brute krachtpogingen te voorkomen; deze kan rekening houden met het IP-adres. Een code die gevalideerd is, moet van de huidige actieve lijst worden verwijderd. Merk op dat de kans dat een duplicaat aanwezig is onder 1000 actieve codes één op 2 miljoen is; dit zou geen probleem mogen zijn; de impact van zo'n zeer zeldzame gebeurtenis kan worden beperkt door altijd de eerste keer dat een code voorkomt te verwijderen. Indien bruut geweld zou worden vermoed, zou ook kunnen worden nagegaan of alleen de eerste codes van elke periode worden gebruikt (het zou zeldzaam moeten zijn dat codes met een tellerwaarde van meer dan 50 worden uitgegeven en gebruikt, cf. infra).

Volgende informatie wordt bewaard:

Verification Service
R1 (code van 15 cijfers die een bepaalde test (en het resultaat daarvan) koppelt aan een mobiel apparaat)
t0 (datum waarop de gebruiker vermoedelijk besmettelijk is geworden)
t3 (datum waarop de resultaten gedownload werden)
test resultaat (positief / negatief)
test channel (lab / arts)
AutorisatieCode AC (digitale handtekening) - tijdelijk bewaard tot voor het inzenden (submission service)

Submission Service
AuthorisatieCode AC (digitale handtekening ter validatie van de beveiligde sleutels)
TEK: beveiligde sleutel
Landen voor TEK
Distribution Service
Opgeladen TEKs (bewaartijd van 14 dagen, zowel de relevante als de dummy TEKs)
Keys en Certificates
• Signing Sleutel die door de distributiedienst wordt gebruikt om de diagnosesleutels te ondertekenen • Public key voor TLS verbinding met de gegevensbank

Voor een gedetailleerde veiligheidsanalyse kan verwezen worden naar https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Upload%20Authorisation%20Analysis%20and%20Guidelines.pdf section 3 - Data Bound Auth Codes.

Geselecteerde beveiligingscontroles in AWS

AWS public cloud biedt een scala aan veiligheidscontroles om gegevens te beschermen tegen ongeoorloofde toegang, wijziging of verwijdering.

Hieronder bevindt zich een lijst van beveiligingsdiensten die voor de backoffice omgeving gebruikt worden. De beveiligingscontroles zijn gegroepeerd per type dienst volgen de structuur van de AWS *Overview of Security Processes* whitepaper, en die zich richten op de diensten die voor de oplossing worden gebruikt. Meer gedetailleerde informatie is te vinden in de whitepaper en op het AWS-documentatieportaal.

- Infrastructuur Security
- Compute diensten
- Network diensten
- Storage diensten
- Database diensten
- (Applicatie beheer - niet van toepassing)
- Deployment en Management Services

Meer informatie kan gevonden in de documentatie beschikbaar over de geselecteerde AWS security controls voor de serverinfrastructuur.

De te beschermen gegevens bestaan uit de Coronalert beveiligde sleutels en de testresultaten van een gebruiker (publieke informatie).

Organisatorische maatregelen Sciensano

Enkel een beperkt aantal Sciensano medewerkers heeft toegang tot de betrokken gegevensbanken. Alle interne en externe medewerkers, tijdelijk of langdurig, hebben een Non-Disclosure Agreement (NDA) met Sciensano getekend.

5.2. Informatieveiligheid app

De app is gebaseerd op het principe van DP-3T welke reeds voorziet in een sterke bescherming van de privacy van de gebruikers. Minstens volgende punten worden opgenomen in de veiligheidsvereisten van de app:

- Toepassing van de principes van DP-3T
- Communicatie tussen app en servers dient geëncrypteerd te zijn
- Informatie wordt degelijk gewist na de voorziene verwerkingstijd
- Bescherming van de confidentialiteit, integriteit zodat sleutels en authenticatiemiddelen beschermd zijn tegen datalekken naar of aanpassing door andere toepassingen op het toestel en hackers.

De onderliggende infrastructuur van de app is de smartphone/gsm waarop de app wordt geïnstalleerd. De gebruiker zal minstens moeten geïnformeerd worden over de risico's die hiermee gepaard gaan.

5.3. Controle op de informatieveiligheid

De aanbesteding voor de ontwikkeling van de app voorziet ook een luik "Audit van de veiligheid". (Lot 2 : Audit de sécurité de l'application et du back office développés dans le Lot 1 van de aanbesteding "Procédure négociée sans publication préalable Smals-BB-001.031/2020").

De audit moet een inschatting maken voor aanvullende beoordelingen van de nood tot bugfixes en het patchen van eventuele kwetsbaarheden.

O.a. volgende objectieven worden beoogd door de audit:

- De mobiele applicatie moet worden geaudit op de integriteit van de gegevens (at-rest of in-motion), zodat de manipulatie van de gegenereerde sleutels, of de validatie van de testcode niet kan worden misbruikt om valse COVID-19 infecties en manipulatie of verwijdering van de opgeslagen sleutels (op de mobiele of op de centrale architectuur) te genereren.
- De audit moet controleren of de toepassing niet gevoelig is voor bekende Bluetooth-gebaseerde aanvalsvectoren.
- De audit moet controleren of de veilige overdracht van infectiegerelateerde sleutels niet kan worden onderschept.
- De audit moet de veilige werking van de mobiele applicatie controleren, met inbegrip van aanvallen op basis van inputvalidatie en inputinjectie.

De vereiste onderdelen van de audit zijn als volgt gedefinieerd:

- Planning
- Security Architecture Review (elke sprint)
- Bedreigingsmodellen (elke sprint)

- Software Compositie Analyse (elke sprint)
- Beoordeling van toepassingsschermen en inputvalidatie (eindaudit)
- Dynamisch Kwetsbaarheidsonderzoek (elke sprint)
- Statische analyse
- Handmatige codebepaling
- Kwaadaardige code-analyse
- Rapportage

Het resultaat van de audit van de app is publiek beschikbaar: https://coronalert.be/wp-content/uploads/2020/10/Report-Coronalert-Application-Security-Assessment-Public-Report_vFINAL.pdf

5.4. Informatieveiligheid EU Gateway

Gedurende het hele proces van afstemming over het ontwerp en ontwikkeling van contact- en waarschuwingstraceringsapplicaties op niveau van de EU is respect voor de privacy van het grootste belang geweest[14]:

- Een nationale app, die wil aansluiten tot de EU Gateway, verzamelt geen gegevens die kunnen leiden tot het onthullen van de identiteit. De app vraagt niet naar de naam, geboortedatum, adres, telefoonnummer of e-mailadres en kan deze ook niet verkrijgen. De app verzamelt geen geolocatiegegevens, inclusief GPS-gegevens. Ook worden er geen bewegingen bijgehouden.
- De Bluetooth Low Energy code wordt volledig willekeurig gegenereerd en bevat geen informatie over de gebruiker of zijn toestel. Deze code verandert meerdere malen per uur, als extra bescherming.
- Alle gegevens die door de app op een smartphone worden opgeslagen, en alle verbindingen tussen de app en de server, en tussen de servers en de gateway, zijn versleuteld.
- Alle gegevens, of ze nu op het toestel van de gebruiker of op de server zijn opgeslagen, worden gewist als ze niet meer relevant zijn, d.w.z. 14 dagen na de overdracht tussen de app en de server.
- De gegevens worden opgeslagen op beveiligde backend servers, die door de nationale autoriteiten worden beheerd. De gateway maakt gebruik van een beveiligde server, die door de Commissie in haar eigen datacentrum in Luxemburg wordt gehost.
- De EU-regels, met name de algemene gegevensbeschermingsverordening (GDPR) en de e-privacyrichtlijn, bieden de sterkste garanties voor betrouwbaarheid (bv. vrijwillige aanpak, minimalisering van gegevens).
- De apps - en ook de gateway - zijn beperkt in de tijd, dat wil zeggen dat ze alleen zullen bestaan zolang de pandemie voortduurt.
- Het Europees Comité voor gegevensbescherming is over de ontwerprichtsnoeren geraadpleegd en heeft een brief opgesteld waarin het initiatief van de Commissie om een pan-Europese en gecoördineerde aanpak te ontwikkelen, wordt toegejuicht.

[14] Zie onder andere:
https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

Door toepassing van deze beperkingen en maatregelen creëert het gebruik van deze gateway geen bijkomende risico's voor de gebruikers van de app die aangeven in het buitenland te hebben verbleven.

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

Voor de inschatting van privacy-risico's gerelateerd aan de gegevensverkeringen van de Coronalert App maakt deze GEB gebruik van risico-analyse tools van Thomas More-hogeschool en de Kruispuntbank Sociale Zekerheid.

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, volgens onderstaande tabel.

				IMPACT		
				Beperkt	Middelmatig	Groot
				1	2	3
				De rechten en vrijheden van de betrokken zijn volledig gevrijwaard	De rechten en vrijheden van de betrokken worden regelmatig beïnvloed	De rechten en vrijheden van de betrokken worden altijd of toch heel vaak beïnvloed
PROBABILITEIT Wat is de waarschijnlijkheid dat het zal gebeuren?	Onwaarschijnlijk	1	Het event komt niet of alleen **in bepaalde omstandigheden** voor	**Aanvaardbaar** Risico **LAAG** 1	**Aanvaardbaar** Risico **LAAG** 1	**Aanvaardbaar** Risico **MEDIUM** 2
	Waarschijnlijk	2	Het event **kan** op een bepaald moment voorkomen	**Aanvaardbaar** Risico **LAAG** 1	**Aanvaardbaar** Risico **MEDIUM** 2	**ONaanvaardbaar** Risico **HOOG** 3
	Zeer Waarschijnlijk	3	Het event **zal** op een bepaald moment gebeuren	**Aanvaardbaar** Risico **MEDIUM** 2	**ONaanvaardbaar** Risico **HOOG** 3	**ONaanvaardbaar** Risico **EXTREEM** 4

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 Privacyverklaring (app + serverinfrastructuur). Promotiecampagnes voor de app. Media-exposure. Vermelding van de specifieke website www.coronalert.be Bijkomende informatie van de zorgvertrekker aan de gebruiker wanneer een staal wordt afgenomen voor een test.	
Residueel risico	
Ondanks dat de voorgestelde maatregelen een breed gamma aan media afdekt, kan het nog steeds voorkomen dat de gebruiker niet volledig geïnformeerd is en daardoor onwetend instemt met het gebruik van zijn gegevens.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	2
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	
Opmaak van Privacyverklaring (app + serverinfrastructuur). Promotiecampagnes voor de app. Media-exposure. De GBE zal publiek gemaakt worden.	
Residueel risico	
Ondanks dat de voorgestelde maatregelen een breed gamma aan media afdekt, kan het nog steeds voorkomen dat de gebruiker niet volledig geïnformeerd is en daardoor onwetend is over de verschillende verwerkingen.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	2
Risico	LAAG

R03. Geautomatiseerde beslisingen

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 berekent op basis van de ontvangen niet-gepersonaliseerde tijdelijke serienummers en de ontvangen beveiligde sleutels van geïnfecteerde personen of de contacten risicovol zijn. Wanneer dit algoritme niet duidelijk is of niet kan gecontroleerd worden op juistheid, dan kan de betrokkene ten onrechte de melding krijgen dat er een risicovol contact was en daardoor gevraagd worden in quarantaine te gaan.
Maatregelen
Het enige deel van de app waarbij er een automatische beslissing is, gebeurt op de mobiele telefoon. Deze berekening staat transparant beschreven in hoofdstuk 5.3. van de nota "Coronalert: A Distributed Privacy-Friendly Contact Tracing App for Belgium". Dit algoritme is uitgebreid getest door onderzoekers van het DP-3T Consortium, Fraunhofer Institute en RKI Institute. Bijkomend kan de betrokkene, in geval van een melding van risicovol contact, contact opnemen met een arts om een test te ondergaan waardoor de quarantaine kan verbroken worden ten gevolge van een negatief resultaat. De formule binnen het algoritme werd recent aangepast door het Duitse instituut (o.a. op basis van inzichten met betrekking tot de Britse variant van het conavirus). Ook België zal de aangepaste formule integreren in Coronalert.
Residueel risico
Wanneer het voorgeschreven algoritme niet correct wordt toegepast kan de betrokkene alsnog verkeerde informatie krijgen waardoor deze onterecht kan gevraagd worden in quarantaine te

R03. Geautomatiseerde beslissingen	
gaan. Doordat de betrokkene een test kan laten afnemen kan de duur van de quarantaine beperkt worden.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	3
Risico	MEDIUM

D02. Naleving van Doelbinding van de gegevensverwerking

Principe	Gebruik de data voor het doel waarvoor u het hebt verzameld, tenzij er een een uitzonderingen 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

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 gebruik van de app heeft als enige bedoeling deze die vastgelegd is in het “Koninklijk besluit nr. 44 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden 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” en wordt hernomen in het toekomstige Samenwerkingsakkoord. Dit besluit voorziet in de wettelijke grondslag om volgende doelstellingen te verwezenlijken (zie verslag aan de Koning): • in de eerste plaats dient een digitale contactopsporingsapplicatie contacten tussen gebruikers op een geautomatiseerde manier te registreren zonder dat hierbij de identiteit van de gebruikers kan achterhaald worden;

R04. Gespecificeerd doel
• in de tweede plaats dient een digitale contactopsporingsapplicatie de gebruiker waarvan de COVID-19 besmetting is vastgesteld de mogelijkheid te geven om vrijwillig te melden dat hij/zij COVID-19 besmet is, en dit op een geautoriseerde en gecontroleerde manier om eventuele foutieve of valse meldingen te voorkomen; • de melding van de besmetting moet vervolgens toelaten om andere gebruikers die in de periode dat de besmette gebruiker besmettelijk was in contact zijn gekomen met de met COVID-19 besmette gebruiker te verwittigen dat zij zich in de nabijheid van deze besmette persoon hebben bevonden, zonder dat hierbij de naam, locatie of exacte tijdstip van besmetting worden doorgegeven.
Residueel risico
De omschrijving is voldoende duidelijk en werd herhaald in het samenwerkingsakkoord tussen de verschillende overheden waardoor het risico hier beperkt is. De mogelijke impact wordt actief gereduceerd door het wettelijke kader die de doelstellingen omschrijft.
Risicoscore

Probabiliteit na maatregelen	1
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
De toepassing maakt gebruik van niet-gepersonaliseerde tijdelijke serienummers en beveiligde sleutels waarvan enkel de beveiligde sleutels op het centraal systeem terecht komen. Doordat deze sleutels gepseudonimiseerd zijn en daardoor haast niet terug te brengen zijn tot het individu zal de impact voor de betrokkene laag zijn. Voor de uitwisseling van test resultaten wordt een testcode R1 gebruikt die geen gegevens bevat waarmee de informatie kan teruggebracht worden tot de telefoon van de gebruiker of de gebruiker zelf. Hierdoor is de impact van verdere verwerking van deze gegevens beperkt. De verwerkingen op de systemen die gebruikt worden voor het beheren van de bovenvermelde gegevens zijn beperkt tot de verwerkingen voor het platform. In die zin is het duidelijk dat de gegevens die op deze platformen aanwezig zijn enkel kunnen gebruikt worden voor de verwerkingen met betrekking tot de digitale contactopsporing.
Residueel risico
De voorziene maatregelen zorgen voor voldoende beveiliging waardoor zowel probabiliteit als impact beperkt worden.
Risicoscore

Probabiliteit na maatregelen	1
Impact na maatregelen	2
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	
Zoals ook aangehaald in buitenlandse GEB's: i) De bijgehouden gegevens kunnen worden gebruikt voor handhaving van de afstandsregels en sociale bubbels, naast de epidemiologische doeleinden. Indien anoniem (statistisch) kan dit leiden tot socio-economische profilering, met als gevolg selectieve maatregelen die het subject beïnvloeden. Indien persoonspecifiek kan het leiden tot vervolging in het geval van overtreding van de maatregelen, of zelfs verminderde zorg (""deze persoon was dermate nalatig, dat we de beademingsapparatuur gebruiken voor iemand anders""). ii) De infrastructuur opgezet voor contact tracing kan worden ingezet om de relaties van verdachte criminelen in kaart te brengen. Politieke druk kan leiden tot een wetswijziging, die het mogelijk maakt in bepaalde gevallen (zoals het opsporen van terroristische netwerken) de app als hulpmiddel te gebruiken in crimineel onderzoek. De impact op de privacy van de gebruikers is afhankelijk van het technisch ontwerp van de app.	
Maatregelen	
De doeleinden van de app zijn duidelijk omschreven in "Koninklijk besluit nr. 44 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden 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" en worden hernomen in het toekomstige Samenwerkingsakkoord. Bijkomend voorziet de applicatie in pseudonimisering van de informatie door het gebruik van beveiligde sleutels voor het uitwisselen van de contactinformatie. Naast het feit dat deze beveiligde sleutels geen geo-locatie informatie bevatten zullen bovenvermelde risico's beperkt worden doordat contacten enkel vastgesteld worden door de app. Bijkomend worden de gegevens verwijderd na downloaden (testresultaten) of na 14 dagen (sleutels). De contactopsporing wordt lokaal door de app bepaald en niet centraal.	
Residueel risico	
Het gebruik van de app is cruciaal om de verspreiding van het coronavirus zo veel als mogelijk te beperken. Omdat het vertrouwen in de app cruciaal is heeft de wetgever andere doelstellingen uitgesloten.. De technische maatregelen op het platform beperken de impact van verdere verwerking van de gegevens. Deze gegevens zijn immers gepseudonimiseerd en quasi onmogelijk om terug te brengen tot de gebruiker of zijn toestellen. Doordat de gegevens slechts beperkt in tijd beschikbaar zijn is de kans op gebruik van de gegevens buiten het doel beperkt. Doordat de informatie op het centrale systeem geen informatie bevat over contacten wordt de mogelijkheid om deze te gebruiken voor andere doeleinden eveneens beperkt.	
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
De betrokkene dient persoonlijke gegevens te verstrekken die niet relevant zijn voor het opgegeven doel van de verwerking.
Toelichting
De verzamelde gegevens dienen beperkt te zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking”). Dit betekent dat de betrokkene, zelfs wanneer hij instemt met het doorsturen van zijn gegevens, de garantie moet krijgen dat de verstrekte gegevens tot het minimum worden beperkt. De app zelf bestaat uit twee afzonderlijke componenten: een "client"-applicatie die wordt beheerd door de nationale volksgezondheidsautoriteit en de Google/Apple Exposure Notification (GAEN)-service, die op Android-toestellen wordt beheerd door Google en deel uitmaakt van Google Play Services. De informatie die de app verzamelt is omschreven in het lastenboek voor de ontwikkeling van de app. Voor de Google Play Services is het zo dat deze in een "privacy bewuste" configuratie ongeveer elke 20 minuten contact opneemt met de Google-servers, waardoor het mogelijk is om bv. de locatie te volgen via het IP-adres. Daarnaast deelt Google Play Services ook de telefoon IMEI, het serienummer van de hardware, het serienummer van de SIM, het telefoonnummer van de handset, het WiFi MAC-adres en het e-mailadres van de gebruiker met Google, samen met de fijnkorrelige gegevens over de apps die op de telefoon draaien. Deze gegevensverzameling is eigen aan de werking van Android en kan niet vermeden worden zonder alle apps van google uit te schakelen. Het valt op te merken dat google geen toegang heeft tot de gegevens verzameld door de app.
Maatregelen
De specificaties van de app zijn publiek gemaakt en opgenomen in het lastenboek voor de ontwikkeling van de app. De uitgewisselde gegevens betreffen de beveiligde sleutels (tussen app en centrale infrastructuur) en niet-gepersonaliseerd tijdelijk serienummer tussen de toestellen van de gebruikers. Beide types van informatie zijn minimaal nodig voor het bepalen van een risico contact. Het algoritme voor het bepalen van de contacten en het risico van het contact maakt enkel gebruik van deze gegevens die uitgewisseld werden. Bij de registratie van de niet-gepersonaliseerde tijdelijks serienummers zal de app bijkomende informatie registreren (duur en sterkte van het signaal) maar doordat de beveiligde sleutels en niet-gepersonaliseerde tijdelijke serienummers gepseudonimiseerd zijn, is deze informatie quasi niet terug te brengen tot een persoon. Een tweede type gegevens betreft de resultaten van de test die een essentieel onderdeel zijn voor de verwerkingen voorzien door de app en het centrale platform. Voor de werking va de app wordt het principe van de dataminimisatie toegepast. De beschrijving van de toepassing geeft aan welke informatie uitgewisseld wordt. Deze informatie is beperkt tot wat strikt noodzakelijk is voor het registreren van de contacten en de respectievelijke duur en afstand voor de contact tracing.

R07. Verzamelen van irrelevante gegevens	
Bij elke nieuwe versie van de app kijken Google en Apple na of de app geo-locatie informatie verwerkt; als dat zo is, krijgt de app geen toegang tot de Google/Apple Exposure Notification Interface en is zij niet meer functioneel. Voor bv. het gebruik van Android kan de dienst “Google Play Services” niet uitgeschakeld worden. Er is geen specifieke privacy policy beschikbaar, maar in de algemene google privacy verklaring wordt de gebruiker geïnformeerd dat het toestel de informatie verzamelt. Het valt op te merken dat de Coronalert App niet zal werken zonder “Google Play Services”. Google geeft aan dat vanaf Android 11 de locatie-instelling niet langer actief te zijn voor de blootstellingsmeldingen: https://support.google.com/android/answer/9930236?hl=nl	
Residueel risico	
De specificatie van de app werden vastgelegd in verschillende documenten en voorziet in de minimalisatie van verwerkte gegevens. Doordat de app gebruik maakt van onderliggende diensten van het Android platform en daarvoor gebruik moet maken van de Google Play Services kan het niet voorkomen worden dat de leverancier van het besturingssysteem bijkomende informatie verzamelt die niet noodzakelijk is voor de beoogde bewerkingen. Zo zal Google informatie verzamelen over locatie op basis van de GPS positie, IP adressen en WiFi informatie, Bluetooth bakens en sensor informatie. Hierbij dient echter opgemerkt te worden dat de informatie van de app zelf, zoals besmettelijkheid of risicocontacten,niet kenbaar gemaakt wordt.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	3
Risico	MEDIUM

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
Voor het uitwisselen van de testresultaten dient het platform deze informatie te bekomen vanuit een andere database bij Sciensano. Deze gegevens komen enkel met de vermoedelijke datum van besmetting en een geheime code. Deze datum en code bevatten geen informatie die de testresultaten kunnen terugbrengen tot het toestel van de gebruiker of de gebruiker zelf en beperken op die manier de mogelijkheid om de bekomen gegevens voor een ander doeleinde aan te wenden. De uitwisseling van deze gegevens is wel essentieel voor de beoogde verwerking. Voor het opladen van beveiligde sleutels wordt ook gebruik gemaakt van een uitwisseling van geheime codes die niet terug te brengen zijn tot het toestel van de gebruiker of de gebruiker zelf. Ook de uitwisseling van deze codes is essentieel voor de werking van het platform. Beide bovenstaande verwerkingen zijn beschreven in het koninklijk besluit nr. 44 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus

R08. Minimaal gebruik van gegevens
COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano waar ook de beperkingen staan opgesomd en het toekomstige Samenwerkingsakkoord. De app zelf zal een verwerking doen van de bekomen geheime sleutels samen met de niet-gepersonaliseerde tijdelijke serienummers verrijkt met afstand en duur om het contactrisico te berekenen. Deze verwerking is gedocumenteerd en publiek gemaakt. Er worden slechts gegevens verwerkt die essentieel zijn om de contact tracing te laten werken zodat deze de privacy van de betrokkene maximaal kan garanderen.
Residueel risico
De gegevens op de app zijn slechts moeilijk terug te brengen tot natuurlijke personen wat de impact van verwerking van niet-relevante gegevens beperkt alsook beperkt dit zeer sterk de mogelijk om de gegevens te verwerken voor andere doeleinden. Het platform is zo ontworpen dat de kans laag is dat andere dan de voorziene gegevens worden verwerkt. Indien dit zou gebeuren zal het betrokkene daar weinig impact van ondervinden gezien alle gegevens gepseudonimiseerd zijn en de gegevensbanken van het platform geen identificeerbare informatie over contacten bevat.

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
i) Er is een risico op vals positieven door foutieve invoer van de zorgverstrekkers in de database van Sciensano die als authentieke bron dient voor het platform Wanneer een resultaat van de test naar het platform voor digitale contactopsporing werd gekopieerd zal dit niet meer kunnen aangepast worden, noch zal de identiteit van de betrokkene kunnen achterhaald worden. ii) Het BT (bluetooth)-signaal passeert door muren, waardoor buren van een indexpersoon, alsook passagiers in andere treinstellen, personen in nabije auto's, of passanten langs het huis van een indexpersoon, allen onterecht een potentiële blootstelling wordt toegekend.

R09. Volledigheid en juistheid van gegevens
Iii) Er is een risico op onterechte waarschuwingen voor zorgverstrekkers die de Coronalert App gebruiken. Zij komen immers in contact met veel risico-patiënten maar dragen beschermende kledij. iv) Er is een risico op het invoeren van vals positieven door gebruikers wanneer deze zijn sleutels zou opladen. De impact zal er dan in bestaan dat andere gebruikers mogelijks een waarschuwing op risicocontact krijgen zonder dat daar een reden toe is. v) Er is een risico bij het gebruik van de covicode dat deze door een andere persoon wordt gebruikt dan degene die een positieve test heeft afgelegd of dat call centre medewerkers ten onrechte covicodes doorgeven. De opgeladen TEK sleutels zullen dan niet noodzakelijk deze zijn van een besmet persoon. vi) Er is een risico dat bij het gebruik van een covicode de gebruiker een excessief lange periode van besmetting invoert waardoor gebruikers ten onrechte een melding van hoog risico contact kunnen krijgen
Maatregelen
i) Datakwaliteitscontrole door Sciensano. Deze kan enkel op macroniveau gebeuren en niet op individueel vlak van de patiënt. De Risk Assesment Group verspreidde een advies om microbiologen en clinici te helpen bij de interpretatie van een zwakpositief PCR resultaat. Follow-up en objectivering inzake de grootorde van vals-positieve testresultaten alsook communicatie daaromtrent zal binnen de schoot van de Interfederale Groep Testing en Tracing worden opgevolgd. ii) Het DP-3T protocol voorziet in zijn berekening van risicocontacten dat er gebruik gemaakt wordt van afstand en duur van het contact. Hierdoor wordt bijvoorbeeld het probleem van een passerende trein beperkt omdat deze contacten korter zullen zijn dan de voorziene tijd zoals vermeld in de specificaties. Bijkomend zal een BT signaal bij doorgang door muren en wanden van bijvoorbeeld treinstellen verzwakt worden wat vaak zal leiden tot een uitsluiting in de berekening van een risico contact. Er zijn uitgebreide testen en metingen gebeurd om de betrouwbaarheid van de schattingen van duur en afstand zo betrouwbaar iii) De Coronalert app voorziet dat de gebruiker tijdelijk het verzenden en ontvangen van Bluetooth tokens voor contactopsporing kan stopzetten (zonder Bluetooth op de telefoon te desactiveren). Dit kan bijvoorbeeld als iemand in de medische sector met beschermmateriaal besmette patienten behandelt of iemand zijn/haar smartphone in een locker achterlaat in een gemeenschappelijke locker ruimte. iv) De gebruiker kan geen geheime sleutels opladen andere dan degene voor de periode van besmettelijkheid. Dit wordt geregeld door het creëren van een autorisatiecode door het platform wanneer een test positief blijkt te zijn. v) het gebruik van de covicode is eenmalig waardoor de mogelijkheid van misbruik beperkt wordt. Bijkomend is de geldigheid van de code beperkt in de tijd waardoor de mogelijkheid tot verdelen beperkt is. vi) voor dit probleem bestaat er op dit moment geen remediëring. Toch blijft de impact voor andere gebruikers beperkt wanneer zij een melding krijgen van een risicovol contact. De besmetting zal steeds door een test moeten bevestigd worden waardoor de impact van zulks foutieve meldingen beperkt zal zijn.
Residueel risico
i) Doordat de kwaliteitscontrole niet op het niveau van een patiënt kan gebeuren *(enkel door microbiologen en clinici)* is de probabiliteit niet geheel verholpen door de voorgestelde maatregelen. Bijkomend zorgen de beschermingsmaatregelen van het platform ervoor dat een patiënt en gebruiker van de app niet kan gewaarschuwd worden wanneer zijn resultaat fout blijkt te zijn. De impact voor gebruiker alsook andere gebruikers kan zijn dat dezen onterecht worden aangeraden in quarantaine te gaan. Voor de gebruikers die enkel een waarschuwing hebben

R09. Volledigheid en juistheid van gegevens	
gekregen kan de duur van de voorgestelde quarantaine beperkt worden door een COVID test aan te vragen. Desalniettemin zal de gebruiker, wanneer deze zich strikt aan de voorgestelde maatregelen wenst te houden een mogelijk risico ondervinden van nutteloze quarantaine. ii) De probabiliteit van deze kwetsbaarheid is beperkt doordat het algoritme bijkomende parameters verwerkt om tot het besluit te komen of een contact al dan niet risicovol was. iii) De probabiliteit dat een gebruiker ten onrechte codes kan opladen wordt beperkt door het systeem van de autorisatiecode. Indien dat toch gebeurt is de impact voor de risisco-contacten, zijnde tijdelijke quarantaine, niet klein maar gelet op de huidige stand van wetenschap inherent aan alle manieren van contactopsporing (inclusief de manuele contactopsporing) waarbij risico-contacten slechts met een kans 10-15% aanleiding geeft tot besmetting. Onterechte, tijdelijke quarantaine zal dus ook bij digitale contactopsporing maatschappelijke aanvaarding vereisen. Vandaar dat de impact op medium geplaatst wordt. vi) gebruikers kunnen foutieve informatie krijgen m.b.t. risicovolle contacten waardoor ze gevraagd kunnen worden om gedurende korte tijd hun sociale interacties te beperken.	
Risicoscore	
Probabiliteit na maatregelen	2
Impact na maatregelen	2
Risico	MEDIUM

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
De gegevens die beschikbaar zijn op het platform en op het toestel van de gebruiker zullen gebruikt worden om de gebruiker van de app te informeren over eventuele risicovolle contacten. Wanneer deze gegevens niet correct zijn kan een gebruiker foute informatie krijgen over risicovolle contacten. Wanneer een risicovol contact niet als dusdanig wordt ingeschat zal de gebruiker geen test aanvragen en zal ook geen noodzakelijke maatregelen nemen. Wanneer een contact ten onrechte als risicovol wordt ingeschat doordat de gegevens niet accuraat zijn, dan zal de gebruiker een test aanvragen en bij letterlijke opvolging van het advies van de app zichzelf in quarantaine plaatsen zonder dat daar een noodzaak toe is.
Maatregelen
Eenmaal de gegevens in het platform opgeladen zijn, dan kunnen deze, doordat ze gespeudonimiseerd zijn, niet gecontroleerd worden op accuraatheid. Evenzeer bestaat er geen mechanisme dat voorziet dat de gegevens, verzameld door de app op een later tijdstip kunnen gecontroleerd worden. Het concept van de app voorziet dat de ter beschikking gestelde gegevens regelmatig gedownload en geconsumeerd worden. Zelf voorzien de app en het platform ook dat de gegevens na een periode van 14 dagen verwijderd worden.
Residueel risico
Doordat de gegevens voor de verdere verwerking noch op acuraatheid of actueelheid kunnen gecontroleerd worden, blijft het risico op hetzelfde niveau als bij R.09
Risicoscore

R10. Accuraatheid en actueelheid van gegevens	
Probabiliteit na maatregelen	2
Impact na maatregelen	2
Risico	MEDIUM

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: • geheime sleutels • niet-gepersonaliseerd tijdelijk serienummer • resultaten van labo testen beschermd door een code Geen van deze codes, serienummers en sleutels bevatten informatie waardoor de gegevens terug te brengen zijn tot een gebruiker. De vermelde kwetsbaarheid is dus niet van toepassing op deze gegevens. De logs met de activiteiten van een gebruiker kunnen echter wel tot identificatie van de gebruiker leiden en zijn onderhevig aan deze kwetsbaarheid.
Maatregelen
De logfiles kunnen informatie bevatten waardoor de aanbieder van diensten (de verwerker is hier AWS) op basis van een IP adres en gecontacteerde servers informatie kan achterhalen van de gebruiker. De app voorziet daarom in het aanleveren van “dummy” informatie (bv. opladen van valse sleutels) waardoor uit deze activiteit geen conclusie kan getrokken worden. Bijkomend is in het centrale platform voorzien dat er geen combinatie van gegevens mag gebeuren tussen logs (bv. IP adres) en activiteit (bv. bekomen van test resultaat).
Residueel risico
Elke dag zal ongeveer 20% van de gebruikers een vals testresultaat downloaden en daarna een valse beveiligde sleutel opladen (d.w.z. zonder autorisatiecode). Gemiddeld wordt 0.1-0.2% van de gebruikers per dag echt getest. Bij een negatieve test wordt nooit een beveiligde sleutel opgeladen, bij een positieve test meestal (maar niet altijd). Maar dit betekent dat per 100 resultaten er 1 echt resultaat is, en dit resultaat lekt een heel klein beetje informatie; maar in het grote plaatje verdwijnt die informatie in de ruis (groot aantal valse testresultaten).

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. Ontbrekend beleid of mechanisme voor het wissen van data	
Toelichting	
Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is, dient de verwerkingsverantwoordelijke termijnen vast 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.	
Maatregelen	
De gegevens worden bewaard op 2 platformen: • Centraal platform : o Testgegevens : testgegevens worden verwijderd nadat de betrokkene deze heeft gedownload o Beveiligde sleutels : worden verwijderd ten laatste 3 weken na de datum van besmetting. De termijn voor het platform is vastgesteld op 14 dagen. • App : o Niet-gepersonaliseerd tijdelijk serienummer : wordt verwijderd na een periode van 14 dagen. o Beveiligde sleutels : worden verwijderd ten laatste 3 weken na de datum van besmetting. De termijn voor het platform is vastgesteld op 14 dagen. o Bij verwijdering van de app van het toestel van de gebruiker worden de niet-gepersonaliseerde tijdelijke serienummers en de beveiligde sleutels verder bewaard tot de periode van 14 dagen is verstreken. De ontvangen testgegevens worden van het toestel verwijderd wanneer de app wordt gedeïnstalleerd. Alle gegevens, die op beide platformen staan, zijn gespeudonimiseerd of worden beschermd door een code die niet terug te brengen is tot een gebruiker of zijn toestel.	
Residueel risico	
Gezien de specificaties van de app en het platform duidelijke bewaartermijnen bevatten en deze technisch geïmplementeerd moeten zijn is de probabiliteit laag. Doordat de gegevens niet terug te brengen zijn tot een gebruiker of zijn toestel is de impact die een gebruiker kan ondervinden eerder beperkt.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	2
Risico	LAAG

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

R13. Gebruiken van niet-verwijderde gegevens	
Er zijn geen retentieregels bepaald voor het platform en de app die bepalen dat gegevens langer dienen bijgehouden te worden dan nodig voor de verwerking. Dit zou ook geen zin hebben gezien de informatie op beide platformen niet terug te brengen is tot de gebruiker of zijn toestel.	
Maatregelen	
De gegevens opgeslagen op de verschillende platformen zijn gepseudonimiseerd en zeer moeilijk terug te brengen tot de betrokkenen. Het pseudoniem gebruikt om een gebruiker te omschrijven zal ook ofwel dagelijks veranderen voor de geheime sleutel, of éénmalig zijn in geval van de test code.	
Residueel risico	
Gezien de gegevens bijna niet tot een betrokkene zijn terug te brengen is de kans op verwerking met impact op de betrokkene zeer klein, ook wanneer deze gegevens niet zouden verwijderd worden. Doordat een pseudoniem nooit meerdere malen gebruikt wordt voor 1 betrokkene blijft de kans op heridentificatie bij combinatie van gegevens zeer laag. Omdat het over medische gegevens gaat, kan de impact indien bij de verwerking de gegevens toch kunnen teruggebracht worden tot de betrokkene, groot zijn.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	3
Risico	MEDIUM

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
De gegevens zijn op 2 platformen beschikbaar nl. de app en het centrale platform.

R14. Ongeautoriseerde toegang tot gegevens
Voor de app gelden volgende kwetsbaarheden (zoals ook aangehaald in buitenlandse GEB's over de contactopsporingsapplicatie) : i) Applicatiedistributeurs (Google Play, Apple Store) verzamelen metagegevens tijdens de installatie, en de-installatie van de contactopsporings app, als onderdeel van hun businessmodel. Hieronder vallen persoonsgegevens gekoppeld aan de applicatie. ii) niet-gepersonaliseerde tijdelijke serienummers kunnen opgevraagd worden en gelinkt aan een persoon waarna deze getracked kan worden. iii) de smartphone van de gebruiker is niet voldoende beveiligd Voor het centrale platform gelden volgende kwetsbaarheden: i) toegangscontrole naar het platform niet voldoende sterk ii) toegang tot de logfiles (infrastructuur) niet voldoende beveiligd iii) gebrek aan mechanisme om datalekken te detecteren iv) het platform zelf niet voldoende beveiligd Voor de communicatie tussen app en platform dient erover gewaakt te worden dat de gegevens niet kunnen onderschept worden.
Maatregelen
Voor alle informatie die beschikbaar is via het platform en op de apps geldt dat deze steeds gepseudonimiseerd is en heel moeilijk tot de betrokkene is terug te brengen. Voor de app gelden volgende bijkomende maatregelen: • Informatie die de app verzamelt is niet toegankelijk voor de gebruikers • Het niet-gepersonaliseerd tijdelijk serienummer verandert om de 10 minuten waardoor het tracken van een persoon bemoeilijkt wordt. • Er is geen uitwisseling van beveiligde sleutels direct tussen de toestellen. In de behandeling van een vorig risico werd het verzamelen van gegevens door de applicatiedistributeurs besproken. Zoals daar aangegeven is er geen toegang tot de gegevens van de app voorzien voor de applicatiedistributeurs. Voor het centrale platform gelden de veiligheidsmaatregelen zoals voorzien in de architectuur. (Zie beschrijving veiligheidsmaatregelen AWS) De communicatie tussen app en platform gebeurt op een beveiligde manier waardoor de gegevens niet kunnen onderschept worden.
Residueel risico
Ondanks de overeenkomsten met de leveranciers Google en Apple blijft er het risico dat dezen in staat zijn om gegevens, verzameld door de app op regelmatige basis naar hun centrale servers te loodsen. Zoals aangegeven in de bespreking van een vorig risico is het voorzien dat deze leveranciers geen toegang hebben tot deze informatie. Voor zowel de app als het centrale platform bestaat de voornaamste bescherming er in dat de gegevens niet terug te brengen zijn tot een natuurlijk persoon. Bij een eventueel lek zal de impact hierdoor altijd laag of beperkt zijn. Door de voorziene veiligheidsmaatregelen zal ook de probabiliteit laag zijn met uitzondering van slecht beveiligde smartphones. Doordat de data in transit geëncrypteerd is, is de probabiliteit op onderschepping van de informatie klein.

Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	3
Risico	MEDIUM

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	
i) Het IP-adres en andere metadata, alsook MAC-adres en andere apparaat-gegevens, kunnen door de verwerker worden gebruikt om een positief getest persoon te identificeren, alsook hun contactgeschiedenis. ii) bij gebruikers met een beperkt aantal contacten kan heridentificatie gebeuren wanneer één van de contacten een besmetting meldt waarvoor via de app een melding zal gebeuren.	
Maatregelen	
i)Het protocol DP-3T is vooral gericht op de pseudonimisering van de gegevens nodig voor het bepalen van de risicovolle contacten en het bekomen van de resultaten van een test. In het design van het platform is er een scheiding voorzien voor toegang tot de log files met o.a. IP adres en het bekomen resultaat. Met het opladen van “dummy keys” wordt het ook moelijk gemaakt om uit het verkeer conclusies te trekken. Deze mogelijkheid werd reeds in eerdere kwetsbaarheden besproken. ii) Voor personen met een beperkt aantal contacten is het belangrijk dat de persconferenties van de Nationale Crisiscel blijven herhalen dat alle soorten bevolkingsgroepen ongeacht leeftijd, ras, geloof, geslacht, medische voorgeschiedens, … geconfronteerd kunnen worden COVID-19 en dat besmetting slechts tijdelijk is en geen reden mag zijn voor stigmatisering of (blijvende) sociale uitsluiting.	
Residueel risico	
i) Door het pseudonimiseren in het DP-3T protocol wordt de operationele data reeds beschermd. Een residueel risico zit vooral in de data die beschikbaar komt door de bijkomende maatregelen voor de informatieveiligheid. Zo zal bijvoorbeeld een WAF de mogelijkheid bieden om de inhoud van het verkeer te controleren en zal er informatie aan de verwerker doorgegeven worden. Omdat deze veiligheidsmaatregelen bepalend zijn voor de beschikbaarheid van het platform wordt aangeraden deze te houden maar niet noodzakelijk te laten uitbaten door de verwerker. Het is ook mogelijk om met een smartphone en een eigen app heimelijk Bluetooth bakens te verzamelen; die werkt op ongeveer 10-20m, maar door een speciale antenne kan men het bereik vergroten tot 100m. Men zou dit kunnen combineren met een digitale camera om de bakens te koppelen aan gebruikers. Als dan een van die gebruikers besmet is en zijn beveiligde sleutels oplaadt, kan men vaststellen dat die specifieke gebruiker positief getest heeft. Deze acties vergen evenwel veel inspanningen waardoor de probabiliteit eerder als laag wordt ingeschat. ii) Hoewel identificatie in het kader van een klein sociaal netwerk niet volledig valt uit te sluiten en een hoge impact kan hebben, schatten we de probabiliteit inzake stijgingen van stigmatisering door de introductie van de app laag in omwille van de toegenomen kennis over COVID-19 binnen de algemene bevolking.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	3
Risico	MEDIUM

R16. Verlies van gegevens

R16. Verlies van gegevens
Kwetsbaarheid

R16. Verlies van gegevens
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

Doordat er geen voldoende redundantiemaatregelen genomen worden kan bij beschadiging of vernietiging van de gegevens, opzettelijk, door een menselijke fout of door een falen van een toestel het platform tijdelijk niet beschikbaar zijn. De impact voor de betrokkenen is dan dat de resultaten van een test niet kunnen bekomen worden via de tool. De impact op de maatschappij is echter groter omdat deze toepassing ervoor moet zorgen dat burgers beter en sneller geïnformeerd zijn over mogelijke risicovolle contacten. Indien dit wegvalt kan de maatschappij geconfronteerd worden met verscherpte maatregelen om corona uitbraak te verhinderen.
Voor het beperken van dit risico dient vooral gekeken te worden naar de toepassing op het centrale platform en de infrastructuur die dit ondersteunt.
 	
• Toepassing:
  o Aanpassing van software maakt dat de gegevensbanken niet langer leesbaar zijn
  o Grootte van de gegevensbank overschrijdt de limieten van het systeem
  o Broncode van de toepassing verdwijnt
• Infrastructuur
  o De beschikbaarheid van het platform is niet voldoende gegarandeerd
  o De beschikbaarheid van het netwerk is niet voldoende gegarandeerd
  o De capaciteit van het platform is niet voldoende voor een correcte verwerking
  o Het platform wordt aangevallen van buitenaf wat tot onbeschikbaarheid leidt
  o Essentiële onderdelen van het platform falen waardoor de dienst onderbroken wordt en gegevens verloren gaan.
De impact bij verlies van gegevens in de app zal de betrokkene een beperkte impact ervaren. Immers, dit zou betekenen dat de sleutel om op te laden op het platform indien de betrokken besmet zou blijken te zijn niet langer beschikbaar zijn.

Maatregelen
• De gegevens worden beveiligd door middel van een backup met restore point • De dienst wordt geïnstalleerd in 3 availability zones van AWS • Door gebruik te maken van AWS als leverancier kan er bij het platform eenvoudig capaciteit bijgeschakeld worden indien dit nodig is • Backups met Point In Time Recovery • Beveiliging door middel van Web Application Firewall en DDOS mitigatie systemen • Verdeling van belasting d.m.v. load balancers
Residueel risico
De veiligheidsmaatregelen zoals voorzien in de maatregelen beperken de impact van verlies van gegevens. Door het gebruik van verschillende availability zones zal de beschikbaarheid beperkt geïmpacteerd worden bij verlies van 1 availability zone zowel voor compute systemen als voor netwerk systemen. Door het gebruik van backups van de database kunnen verloren gegane gegevens gerecupereerd worden waardoor de beschikbaarheid van het platform en zijn gegevens voor de gebruiker maximaal gegarandeerd blijft en de gevolgen van een outage beperkt wordt. In geval een gebruiker de gegevens van zijn app verliest dan zal deze gebruiker op manuele contactopsporing dienen terug te vallen.
Risicoscore

Probabiliteit na maatregelen	1
Impact na maatregelen	2

R16. Verlies van gegevens	
Risico	LAAG

R17. Detectie van datalekken

R17. Detectie van datalekken	
Kwetsbaarheid	
Er is geen mechanisme dat automatisch datalekken detecteert	
Toelichting	
De gegevens die verwerkt worden bevatten informatie die kan gebruikt worden voor het bepalen van risicovolle contacten (medische informatie) en informatie over de resultaten van de aangevraagde testen. Voor het centraal platform dient er gekeken te worden naar de mogelijke lekken van testresultaten. Voor de app dient gekeken te worden naar de mogelijke lekken van contactinformatie. Eenmaal de geheime sleutels door een gebruiker werden opgeladen zijn deze gegevens publiek. Een lek van deze gegevens betekent geen risico voor de betrokkenen.	
Maatregelen	
Het platform noch de app beschikken over een systeem dat het lekken van data zal detecteren.	
Residueel risico	
Hoewel het lekken van gegevens niet zal gedetecteerd worden zal de impact van een lek vanaf het centraal platform beperkt blijven. De confidentiële data betreft de code die de toegang tot het resultaat van de test beschermt en deze bevat geen informatie die tot de betrokkene of zijn toestel terug te brengen is. Hierdoor is de kans op impact voor de betrokkene klein. Eventuele lekken vanaf een individuele app hebben een beperkte impact gezien het volume, maar vooral doordat dit enkel het niet-gepersonaliseerd tijdelijk serienummer betreft wat als gepseudonimiseerde informatie dient beschouwd te worden en moeilijk terug te brengen is tot een betrokkene.	
Risicoscore	
Probabiliteit na maatregelen	2
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. Gezien het belang van deze maatregelen dienen deze maatregelen op regelmatige tijdstippen getest te worden om hun efficiëntie te meten.
Maatregelen
De belangrijkste maatregel voor de bescherming van gegevens is het toepassing van het DP-3T protocol. Door deze maatregel worden gegevens gepseudonimiseerd en kunnen deze niet teruggebracht worden tot de betrokkene of zijn toestel. Zoals eerder gemeld zal de impact van een lek beperkt worden. Bijkomend zal de architectuur van het platform voorzien in beschikbaarheid over meerdere availability zones en zal een back-up voorzien worden om de beschikbaarheid van het platform

R18. Testen van beveiligingsmaatregelen	
maximaal te garanderen. De bescherming van het platform zelf is voorzien met de veiligheidsdiensten van de verwerker (AWS) De beveiliging van de smartphones kan niet gecontroleerd worden gezien deze onder de verantwoordelijkheid van de gebruiker valt. Tijdens de ontwikkeling van de app en het platform is voorzien dat de ontwikkelaar zowel de functionele als niet-functionele aspecten van de toepassing test. Bijkomend zal een auditeur de ontwikkelde software testen op veiligheidspunten.	
Residueel risico	
De confidentialiteit van de informatie is beschermd door het pseudonimiseren van de gegevens. De architectuur voorziet hierin en het platform wordt getest op kwetsbaarheden na elke release waardoor de kans op incident verminderd wordt. Voor het platform is een regelmatige test ook cruciaal. Bij de release van de software wordt een penetration test voorzien die ook de kwetsbaarheid van het platform test. Er blijft een kwetsbaarheid rond beschikbaarheid, vooral wat betreft fail-over en restore van gegevens.	
Risicoscore	
Probabiliteit na maatregelen	2
Impact na maatregelen	2
Risico	MEDIUM

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	
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	
Maatregelen	
Hoewel het vermijden van lekken en het behandelen van deze lekken moet beschreven worden in een datalekkenbeleid, zorgt het pseudonimiseren van alle informatie er voor dat de gelekte informatie niet tot een natuurlijk persoon kan teruggebracht worden. Doordat de informatie gepseudonimiseerd is en de verwerkingsverantwoordelijke van het centrale platform de gegevens niet kan terugbrengen tot een natuurlijk persoon, zal er geen individuele waarschuwing kunnen komen voor de betrokkenen van wie gegevens werden gelekt. Beide opmerkingen zijn van toepassing voor zowel de opgeladen geheime sleutels als voor de testresultaten. Het valt op te merken dat de geheime sleutels publieke informatie zijn zodra deze opgeladen zijn. Bij een lek is er geen impact voor deze laatste gezien het reeds een publiek gegeven is.	
Residueel risico	
Het residueel risico voor de betrokkene is vooral het lekken van medische informatie waarvoor deze niet kan gewaarschuwd worden. Echter, doordat de informatie gepseudonimiseerd is, is de impact voor de betrokkene beperkt en kan het risico als laag ingeschat worden.	
Risicoscore	
Probabiliteit na maatregelen	1

R19. Procedure Datalekken	
Impact na maatregelen	2
Risico	LAAG

R42. Blootstelling van gegevens aan derden

R42. Blootstelling van gegevens aan derden	
Kwetsbaarheid	
Gegevens die niet vallen onder het contactonderzoek worden blootgesteld aan derden als gevolg van de ingebruikname van de applicatie.	
Toelichting	
Zoals ook aangehaald in buitenlandse GEB's over contactopsporingsapplicaties: i) Het permanent inschakelen van Bluetooth (BT), geeft hackers de mogelijkheid bestaande, gekende BT-veiligheidslekken te misbruiken - geautomatiseerde inbraak via deze lekken is mogelijk wanneer een aanvaller en het doelwit op korte afstand zijn. De laatste (en veiligste) versie van Bluetooth kan niet vereist worden, omdat dat gebruikers uitsluit. ii) Winkelcentra, vliegvelden, stations, en dergelijken zijn reeds uitgerust met een BT-trackinginfrastructuur om gedrag van klanten te volgen, zoals lengte van verblijf, route door het pand, en terugkeerpercentage. Personen die de Coronalert App ingeschakeld hebben zijn niet in staat hun BT uit te schakelen, waardoor grote hoeveelheden gegevens in handen kunnen komen van derde instanties.	
Maatregelen	
De kwetsbaarheden van het gebruik van Bluetooth als middel om het niet-gepersonaliseerd tijdelijk serienummer uit te wisselen zijn eigen aan het gebruik van Bluetooth en niet van de app. In die zin kunnen er geen extra maatregelen voorzien worden in de app om deze kwetsbaarheden weg te werken. Het "Koninklijk besluit nr. 44" en het Samenwerkingsakkoord voorzien dat een burger op geen manier kan verplicht worden om de app te installeren. Wanneer de burger dit risico als groot inschat kan deze dus beslissen de app niet te installeren.	
Residueel risico	
Het risico zoals hierboven beschreven kan niet verholpen worden met de app. De enige maatregel om deze kwetsbaarheid weg te werken is het uitschakelen van de app. Het risico op tracking d.m.v. Bluetooth is aanwezig bij het gebruik van de app, net zoals dit risico aanwezig is bij het gebruiken van audiosets verbonden via Bluetooth.	
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
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. Wettelijk kader werd opgemaakt op Federaal en Gewest en Gemeenschapsniveau. Dit bestaat uit het koninklijk besluit nr. 44 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden 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 en werd verder uitgewerkt in een Samenwerkingsakkoord tussen de verschillende beleidsniveaus. Gezien de bestrijding van corona van algemeen belang is voor de volksgezondheid en een grensoverschrijdend belang heeft, is het verbod op verwerken van medische gegevens niet van toepassing. Bijkomend, wordt de gebruiker bij het installeren van de app en bij het uitwisselen van de gegevens instemming gevraagd voor het verder verwerken van deze gegevens zonder dat dit noodzakelijk is voor de rechtmatigheid van de verwerking.
Residueel risico
Doordat de finaliteit van de verwerking een rechtmatige rechtsgrond voorziet volgens de AVG, het belang voor de volksgezondheid van deze verwerkingen die een opheffing van het verbod op het verwerken van medische gegevens voorziet en de verschillende KB's en overeenkomsten tussen de verschillende beleidsniveaus is de kans dat deze kwetsbaarheid optreedt zeer beperkt. De impact van het niet respecteren van deze vereiste is matig tot groot gezien de verwerking dan niet langer

R20. Rechtmatigheid van verwerking	
kan doorgaan en burgers niet op tijd zullen gewaarschuwd worden voor een eventueel risicovol contact. Aangaande de continuïteit van het wetgevend kader, valt niet uit te sluiten dat bepaalde onderdelen naar aanleiding van hangende rechtsprocedures vernietigd worden. In dat geval kan verwacht worden dat wet- of regelgevers eventuele gebreken (snel en/of retroactief) zouden herstellen omwille van het ruime maatschappelijke en politieke draagvlak voor proportionele maatregelen in strijd tegen COVID-19.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	2
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
De rechtmatigheid van de verwerking is gebaseerd op artikel 6.1.e van de AVG en het verbod op verwerken van medische gegevens wordt opgeheven door inroeping van artikel 9.2.i van de AVG. Bijgevolg is er geen verdere toestemming nodig van de betrokkenen voor het verwerken van de gegevens.
Maatregelen
Er worden geen bijkomende maatregelen genomen.
Residueel risico
Doordat de rechtmatigheid van de verwerking wordt bekomen uit 6.1.e van de AVG is de probabiliteit hier zeer laag.
Risicoscore

Probabiliteit na maatregelen	1
Impact na maatregelen	2
Risico	LAAG

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 deze toepassing ligt in het beschermen van de volksgezondheid wat geldt als een voldoende reden vermeld in 9 §2.i waardoor het verbod iet van toepassing is.
Maatregelen

R22. Legitimiteit verwerking bijzondere categorieën persoonsgegevens	
Bijkomend bij de uitzondering vermeld in AVG artikel 9 §2.i wordt ook bij elke uitwisseling van gegevens aan de gebruiker de instemming gevraagd om de gezondheidsgegevens te verwerken.	
Residueel risico	
Het initiële risico is reeds laag doordat het belang van de volksgezondheid een opheffing van het verbod op verwerking van medische gegevens verrechtvaardigt. Doordat de gebruiker ook nog expliciet om zijn instemming wordt gevraagd bij de uitwisseling van de gegevens en de verdere verwerking ervan dient het risico als laag te worden ingeschat.	
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	
De infrastructuur noch de app voorziet in het verwerken van juridische informatie.	
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	
Er wordt bij de installatie van de toepassing op een smartphone niet nagegaan wat de leeftijd van de gebruiker is. Op die manier kunnen kinderen die over een mobiel toestel beschikken de app installeren waardoor hun persoonsgegevens alsnog verder verwerkt worden door andere gebruikers en door het centrale platform. De beoogde verwerkingen zijn niet specifiek gericht op kinderen waardoor de verstrekte informatie niet noodzakelijk in een taal zal gebeuren die volledig verstaanbaar is voor kinderen. (Recital 58 AVG)	
Maatregelen	
De AVG voorziet dat, wanneer gegevens van kinderen worden verwerkt, deze kinderen met betrekking tot hun persoonsgegevens recht hebben op specifieke bescherming, aangezien zij zich allicht minder bewust zijn van de betrokken risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van persoonsgegevens.	

R24. Verwerking gegevens van minderjarigen	
De app en het centrale platform zijn zo geconcipiëerd dat deze voorzien in voldoende bescherming van de gegevens, ook als deze van kinderen afkomstig zijn. De website www.coronalert.be bevat laagdrempelige informatie die ook begrijpelijk is voor jongeren. Indien er op basis van de ontvangen vragen rond Coronalert (of andere signalen) een noodzaak zou blijken om de communicatie aan te passen ten aanzien van jongeren dan zal een aangepaste informatiestrategie in overweging worden genomen.	
Residueel risico	
De app en het platform voorzien in voldoende maatregelen om de gegevens van kinderen afdoende te beschermen. Net zoals voor andere bevolkingsgroepen geldt dat bij kinderen met weinig sociale contacten er een risico op heridentificatie is wanneer deze een bemetting zou rapporteren in het systeem. De probabiliteit wordt op 2 ingeschat voor deze laatste categorie van kinderen en hoewel de impact bij R.15 op 3 werd geschat zal deze voor de kinderen op 2 worden ingeschaald omdat hier van de veronderstelling wordt uitgegaan dat deze kinderen hun contacten zullen hebben binnen de beslotenheid van een groep van vertrouwenspersonen.	
Risicoscore	
Probabiliteit na maatregelen	2
Impact na maatregelen	2
Risico	MEDIUM

R43. Gebruik applicatie 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. kunnen toegangsrestricties invoeren voor mensen die de app niet geïnstalleerd hebben
Maatregelen
Het charter van de app stelt het volgende: *De app mag niet leiden tot enige vorm van individuele discriminatie.* Het koninklijk besluit nr. 44 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden 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 voorziet dat het de burger toekomt om de beslissing te nemen deze toepassing al dan niet te installeren en te gebruiken en de gegevens door te sturen in geval van een besmetting Meer specifiek bepaalt het KB dat “Op aanbeveling van de GBA in haar advies 34/2020 wordt ook verduidelijkt dat een (niet-) gebruiker op geen enkele manier een nadeel of een voordeel mag ondervinden op grond van het al dan niet gebruiken van een digitale contactopsporingsapplicatie”. Het Samenwerkingsakkoord vermeldt het volgende: Het opleggen door een overheid, bedrijf of individu aan een ander individu tot het verplicht installeren, gebruiken en de-installeren van de digitale contactopsporingsapplicatie zal bestraft worden op grond van de gemeenrechtelijke straffen (verbod op discriminerende handelingen, verbod op onrechtmatige gegevensverwerking,…).
Residueel risico

R43. Gebruik applicatie onder dwang	
Het KB en het Samenwerkingsakkoord benadrukken het bestaan van bescherming waardoor de kans dat een burger gedwongen wordt deze toepassing te installeren beperkt wordt.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	2
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.
Maatregelen
Voor verwerking wordt een privacy notice opgesteld. Deze omvat de noodzakelijke informatie over de verwerking en de verwerkingsverantwoordelijke zoals aangegeven in de AVG. Bijkomende wordt aan het publiek informatie ter beschikking gesteld via volgende websites : • https://www.corona-tracking.info/app/coronalert/ • https://www.esat.kuleuven.be/cosic/sites/corona-app/
Residueel risico
Hoewel de informatie over de app rijkelijk aangeboden wordt via verschillende kanalen bestaat steeds de kans dat deze bepaalde groepen van de bevolking en de gebruikers niet zal bereiken doordat ofwel de kanalen niet gekend zijn of doordat de informatie niet eenvoudig te begrijpen is. Om die reden wordt aangeraden verder te werken op eenvoudige omschrijving van alle nodige en relevante informatie wanneer de gebruiker gevraagd wordt in te stemmen metde installatie van de app en de handelingen voordoorsturen van informatie.

R25. Toelichten impact gegevensverwerking	
Door de controles van de verschillende organen bij het ontwikkelen van de app en het centraal platform, en de maatregelen die voorzien zijn ter bescherming van de vertrouwelijkheid van de gegevens en privacy van de gebruiker is de impact eerder beperkt.	
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 app, de verwerkingen die plaatsvinden en de gegevens die hiervoor gebruikt worden.	
Maatregelen	
De informatie wordt in zo eenvoudig mogelijke bewoordingen ter beschikking gesteld via de verschillende kanalen (zie R.25). Communicatiekanalen worden opgelijst en zo veel mogelijk in gebruik genomen.	
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. Om die reden wordt aangeraden verder te werken op eenvoudige omschrijving van alle nodige en relevante informatie wanneer de gebruiker om instemming gevraagd wordt voor de installatie van de app en bij het doorsturen van informatie. Door de controles van de verschillende organen bij het ontwikkelen van de app en het centraal platform, en de maatregelen die voorzien zijn ter bescherming van de vertrouwelijkheid van de gegevens en privacy van de gebruiker is de impact eerder beperkt.	
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 enkel persoonsgegevens van een betrokkene bekomen via het platform van Sciensano via dewelke de resultaten van de test worden meegedeeld aan het platform.
Maatregelen
De verwerkingverantwoordelijke van het platform is Sciensano. Sciensano voorziet ook in het verstrekken van de resultaten van de testen aan het platform dat de gegevens ter beschikking stelt

R27. Informatie over aanvullende gegevens	
van de app. De privacy notice, de informatie over de app en het KB met de samenwerkingsakkoorden voorzien ook in de vereiste informatie.	
Residueel risico	
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	
Om redenen van algemeen belang op het gebied van de volksgezondheid is het nodig om gezondheidsgegevens van de betrokkene te verwerken. Deze verwerking moet daarom worden onderworpen aan passende en specifieke maatregelen ter bescherming van de rechten en vrijheden van natuurlijke personen. Dergelijke verwerking van persoonsgegevens over gezondheid om redenen van algemeen belang mag er niet toe te leiden dat persoonsgegevens door derden zoals werkgevers, of verzekeringsmaatschappijen en banken voor andere doeleinden worden verwerkt. In dit geval dient rekening gehouden te worden met doorgifte van geheime sleutels naar landen binnen de Europese Economische Ruimte waar bij de verwerking van de gegevens bijkomende verwerkingsverantwoordelijken zullen geïdentificeerd worden.	
Maatregelen	
Het wettelijk kader (KB nr. 44, Samenwerkingsakkoord)bepaalt de doelstellingen van de verwerking en verbiedt de verwerking van de verzamelde gegevens voor andere doeleinden. Hierdoor is doorgifte aan derden niet toegestaan. De app maakt het mogelijk dat sleutels kunnen worden uitgewisseld met andere Europese landen, mits de gebruiker de landen aangeeft waar hij verbleven heeft tijdens de periode van besmettelijkheid. Dit impliceert dus een goedkeuring van de gebruiker voor de export van deze sleutels. De uitwisseling van de sleutels zal enkel gebeuren met de landen die ook gebruik maken van het DP-3T protocol. De uitwisseling is voorzien op basis van gepseudonimiseerde gegevens. De verwerkingsverantwoordelijken die deze gegevens verder zullen ontvangen zijn nationale gezondheidsinstanties binnen de Europese Economische Ruimte voor de beheer en uitbaten van de nationale Corona tracking app enerzijds en het coördinerende orgaan binnen de Europese instellingen voor het opzetten en uitbaten van de Europese gateway voor het uitwisselen van de informatie m.b.t. de besmettingen.	
Residueel risico	
Het wettelijk kader voorziet in voldoende waarborgen opdat de informatie niet met derden, anders dan de gezondheidsinstanties binnen de Europese landen wordt uitgewisseld waardoor de kans hierop klein is. Bijkomend beschikt het platform enkel over gepseudonimiseerde informatie waardoor de gegevens moeilijk kunnen teruggebracht worden tot de natuurlijke persoon en de impact van zo een uitwisseling klein is.	
Risicoscore	
Probabiliteit na maatregelen	1

R28. Informatie over derde dataverwerkers	
Impact na maatregelen	1
Risico	LAAG

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.
Maatregelen
Sciensano heeft 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.
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. Om die reden wordt aangeraden verder te werken op eenvoudige omschrijving van alle nodige en relevante informatie wanneer de gebruiker gevraagd wordt om in te stemmen metde installatie van de app en met het doorsturen van informatie. Door de controles van de verschillende organen bij het ontwikkelen van de app en het centraal platform, en de maatregelen die voorzien zijn ter bescherming van de vertrouwelijkheid van de gegevens en privacy van de gebruiker is de impact eerder 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 architectuur van dit platform voorziet dat alle informatie gepseudonimiseerd wordt verwerkt, zonder dat de verwerkingsverantwoordelijke over de mogelijkheid beschikt deze informatie terug te brengen tot de betrokkene of zijn toestel.

R30. Geïndividualiseerde informatie over verwerkte gegevens	
Artikel 12 §2 van de AVG stipuleert" De verwerkingsverantwoordelijke faciliteert de uitoefening van de rechten van de betrokkene uit hoofde van de artikelen 15 tot en met 22. In de in artikel 11, lid 2, bedoelde gevallen mag de verwerkingsverantwoordelijke niet weigeren gevolg te geven aan het verzoek van de betrokkene om diens rechten uit hoofde van de artikelen 15 tot en met 22 uit te oefenen, tenzij de verwerkingsverantwoordelijke aantoont dat hij niet in staat is de betrokkene te identificeren." Door de pseudonimisatie van de gegevens kan de verwerkingsverantwoordelijke de betrokkene niet identificeren waardoor deze vereiste niet van toepassing is.	
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
De behandelend arts van de betrokkene en het labo, dat de test uitvoert, verzenden in het kader van de testresultatenserver (gegevensbank VI) een beperkt aantal persoonsgegevens van de betrokkene naar Sciensano. Conform artikel 16 AVG heeft de betrokkene de mogelijkheid deze gegevens te verbeteren.
Maatregelen
Indien de gegevens door de behandelend arts en labo reeds verzonden en verwerkt zijn, kunnen deze gegevens omwille van pseudonimisatie niet meer verbeterd worden binnen gegevensbank VI door Sciensano. Zie ook de aangehaalde problematiek rond vals-positieven. Het nemen van bijkomende maatregelen is gelet op de automatisering van de processen voor de testresultatenserver en de noodzaak om in het kader van een effectieve bestrijding van de verspreiding van COVID-19 snel tot waarschuwingsacties te komen, niet mogelijk.

R31. Wijzigen van gegevens	
Deze beperking inzake het recht op rectificatie zal vermeld worden in de privacyverklaring zodat de betrokkene hiervan op de hoogte is en eventueel zelf kan beslissen (in het geval van een vermoeden van incorrecte informatie) om geen actie voor waarschuwingen te ondernemen.	
Residueel risico	
Omwille van pseudonimisatie zijn er belemmeringen om het recht op rectificatie uit te laten voeren door de verwerkingsverantwoordelijke. Indien de betrokkene fouten vermoedt, kan hij er evenwel voor kiezen om geen sleutels op te laden naar gegevensbank V zodat foutieve waarschuwingen vermeden kunnen worden. Hierdoor kan de betrokkene zelf een negatieve impact voor anderen beperken.	
Risicoscore	
Probabiliteit na maatregelen	2
Impact na maatregelen	2
Risico	Medium

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	
Er worden geen gegevens uitgewisseld met derden door de beperkingen die opgelegd worden door het KB (geen bijkomende verwerking anders dan de doeleinden bepaald in het KB voor de app). Voor de uitwisseling van sleutels met derde landen is er, doordat de gegevens gepseudonimiseerd zijn, geen mogelijkheid om de identiteit van de betrokkene te achterhalen en dus geen mogelijkheid om deze gegevens te corrigeren.	
Maatregelen	
Via de privacyverklaring zullen de betrokkenen geïnformeerd worden dat er op vlak van derden enkel met EER landen gegevensuitwisseling mogelijk is. In diezelfde privacyverklaring zullen de betrokkenen kunnen lezen dat er belemmeringen zijn inzake rectificaties.	
Residueel risico	
Indien de betrokkene fouten vermoedt, kan hij er evenwel voor kiezen om geen sleutels op te laden naar gegevensbank V zodat foutieve waarschuwingen vermeden kunnen worden. Hierdoor kan de betrokkene zelf een negatieve impact voor anderen beperken	
Risicoscore	
Probabiliteit na maatregelen	2
Impact na maatregelen	2
Risico	MEDIUM

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	
Indien er een andere app-aanbieder zou zijn, dan kan men oordelen dat de betrokkene zijn persoonsgegevens zou kunnen laten overdragen naar deze aanbieder.	
Maatregelen	
Irrelevant: geen andere app voor overdracht beschikbaar. Google en Apple laten maar aan 1 app toe per land/regio om gebruik te maken van de Google/Apple Exposure Notification API. Risico kan geherevalueerd worden indien Google en Apple hun regels zouden veranderen en er een andere app-aanbieder zich zou aanbieden en details over diens werkwijze bekend zouden zijn: o.a. welke gegevens zal hij/zij exact (mogen) gebruiken?	
Residueel risico	
Niet van toepassing (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 gegevens van de betrokkene worden niet verwerkt op zodanige basis dat deze tot een automatische beslissingsprocedure leidt. Het resultaat van de verwerking is een melding of de betrokkene al dan niet een risicovol contact heeft gehad waarbij in het positieve geval wordt aangeraden in quarantaine te gaan en een covid test te laten afnemen. Om deze reden is dit artikel niet van toepassing.	
Maatregelen	
Niet van toepassing	
Residueel risico	
Niet van toepassing	
Risicoscore	
Probabiliteit na maatregelen	NVT
Impact na maatregelen	NVT

R34. Bezwaar tegen beslissingsprocedures	
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 van de app (KB nr. 44, Samenwerkingsakkoord van 25 augustus 2020)bepaalt de doelstellingen van de verwerking en verbiedt de verwerking van de verzamelde gegevens voor andere doeleinden. Hierdoor is doorgifte aan derden niet toegestaan en is dit artikel niet van toepassing. Enkel overdracht van het niet-gepersonaliseerd tijdelijk serienummer aan een andere gebruiker van de app is voorzien. Dit gebeurt gepseudonimiseerd en is omschreven in de privacy notice.	
Maatregelen	
Niet van toepassing (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. In deze betreft het een toepassing waarbij gegevens bij de betrokkene worden verzameld en de betrokkene instemt vooraleer deze naar het platform te sturen. Voor de gegevens bekomen uit de authentieke bron bij Sciensano dient de gebruiker ook zijn instemming te geven vooraleer deze kunnen gegenereerd worden. Voor het gebruik van de app dient de gebruiker zijn instemming te geven bij de installatie. Algemeen kan gesteld worden dat de verwerking pas zal gebeuren nadat de gebruiker hiermee apart instemt en het bezwaar niet verder nuttig is. Mocht de gebruiker alsnog beslissen om bezwaar aan te tekenen na het geven van een instemming, dan zal de verwerkingsverantwoordelijke hier niet positief kunnen op reageren. Immers door de pseudonimisatie zullen de gegevens niet langer terug te brengen zijn tot de betrokkene en daarom niet van het platform kunnen verwijderd worden. Om bovenstaande redenen wordt geacht dat dit recht niet kan uitgeoefend worden.	
Maatregelen	
Rechten van de betrokkene zijn beschreven in de privacyverklaring	
Residueel risico	
Omwille van pseudonimisatie zijn er belemmeringen om deze rechten te kunnen uitvoeren. Doordat de gebruiker expliciet moet instemmen met de verwerking is de kans dat dit voorkomt eerder laag. De gebruiker is via de privacy notice geïnformeerd over de beperkingen om bezwaar	

R36. Bezwaar tegen verwerking van persoonsgegevens	
uit te oefenen. Omdat dit een apart document is dat aan de aandacht van de gebruiker kan ontsnappen is het ook aangeraden deze melding te geven bij elke instemming d e gevraagd wordt. De impact wordt beperkt door de pseudonimisatie waardoor de identiteit van de betrokkene zeer moeilijk te achterhalen is. Bijkomend worden de gegevens gewist na een periode van 14 dagen waardoor de impact in tijd beperkt is.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R37. Informeren over bezwaar verwerking van persoonsgegevens

R37. Informeren over bezwaar verwerking van persoonsgegevens	
Kwetsbaarheid	
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	
Zoals aangegeven in eerdere hoofdstukken worden er geen gegevens uitgewisseld met een derde partij die deze gegevens verwerkt met impact op de betrokkene. Wel wordt het niet-gepersonaliseerd tijdelijk serienummer uitgewisseld met andere gebruikers van de app die op basis van deze gegevens bepalen of er een risicovol contact heeft plaatsgevonden.	
Maatregelen	
De app vereist dat de gebruiker bij het installeren van de app op de smartphone zijn instemming geeft. Bijkomend is de informatie beschikbaar over de doelstellingen van de app en de informatie die uitgewisseld wordt. Vooraleer de betrokkene zijn geheime sleutels naar het platform doorstuurt en vooraleer hij een R1 testcode aanmaakt voor het verkrijgen van de resultaten van een test, dient de gebruiker zijn expliciete toestemmng te geven.	
Residueel risico	
Doordat de gebruiker instemt bij het installeren van de app en bij het uitwisselen van gegevens is de kans beperkt dat er bezwaar wordt gemaakt tegen verdere verwerking van deze gegevens. Echter, wanneer de gebruiker alsnog bezwaar wenst aan te tekenen tegen de verwerking van zijn gegevens, dan kan door de pseudonimisatie van deze gegevens geen positief gevolg hieraan gegeven worden. Doordat de gegevens gepseudonimiseerd zijn en beperkt beschikbaar in de tijd zal de impact van de negatieve respons op de vraag tot staking van de verwerking klein zijn.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

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

Er worden geen individuele besluiten genomen die impact hebben op de betrokkene die zijn informatie ter beschikking stelt. De resultaten zijn ofwel het gevolg van een test ofwel het medelen van informatie op basis van een conclusie op risicovol contact die de betrokkene aanraden om bepaalde maatregelen te handhaven. De risico's verbonden met deze laatste werden reeds behandeld in R.03.

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 veiligheidsmatregelen.
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
Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens en de mate waarin zij worden verwerkt.
Maatregelen
Het DP-3T protocol werd volgens deze principes uitgewerkt (en werd getoetst door European Data Protection Board) en wordt toegepast in de app en het ondersteunende platform. Bijkomende technische maatregelen zoals encryptie voor data in rest en data in transit voorzien in bijkomende veiligheidsmaatregelen. De mogelijke en toegestane verwerkingen zijn duidelijk omschreven en zijn beperkt in het KB. Bijkomende verwerkingen zijn niet toegestaan en door de pseudonimisatie voorzien in het DP-3T protocol zijn deze ook niet mogelijk of niet zinvol omdat het resultaat ervan bijna niet terug te brengen is tot een natuurlijk persoon. De toepassing voorziet in dataminimisatie door het ontwerp van DP-3T. De gebruiker dient enkel zijn goedkeuring te geven voor het gebruik van de app. Er wordt verder niet gevraagd aan de gebruiker om privacy instellingen te configureren.
Residueel risico
Door de toepassing van DP-3T en de toepassing van de vooropgestelde veiligheidsmaatregelen is de toepassing van bij het ontwerp voorzien op de bescherming van de rechten van de betrokkenen die de toepassing gebruiken. Om die reden is de kans dat misbruik gemaakt wordt van de gegevens verzameld voor de beoogde verwerkingen klein.

R38. Privacy by design and by default	
Doordat de instellingen niet kunnen aangepast worden, wordt ook de mogelijkheid op fouten door de gebruiker geminimaliseerd.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

D14. Naleven van organisatorische verplichtingen

Principe	0
Samenvatting	0
Link AVG	0

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
De verwerkingsverantwoordelijke wordt geacht de instructies op te stellen voor de verwerker die de gegevens verwerkt in opdracht van de verwerkingsverantwoordelijke. Voor dit platform zal Amazon Web Services (AWS) het platform aanleveren. De ontwikkelaar van de app en het platform zal niet instaan voor het beheer van het platform. Om de leverancier de mogelijkheid te bieden tussen te komen op het platform werd in het lastenboek een vertrouwelijkheidsclausule voorzien (4.2.37 - 4.2.42 van het lastenboek https://www.corona-tracking.info/wp-content/uploads/2020/07/Smals-BB-001-031-2020.pdf) In het kader van dergelijke tussenkomsten werd er dan ook een overeenkomst afgesloten met deze leverancier.
Maatregelen
De verwerkingsverantwoordelijke voorziet in het afsluiten van een verwerkersovereenkomst met zijn verwerker.
Residueel risico
Door het afsluiten van een verwerkersovereenkomst en de bijkomende maatregelen is de kans op inbreuk tegen deze regel klein. Echter, wanneer de verwerker zich niet aan deze overeenkomst houdt, dan kan dit impact op het individu hebben doordat gegevens beschikbaar komen van de verwerker. Door de opgelegde scheiding van databanken en logfiles in het design wordt deze impact beperkt, maar er blijft wel de mogelijkheid tot identificatie aan de hand van het IP adres en bepaling van inhoudelijke informatie door de sequentie van activiteiten van een gebruiker.

Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	2
Risico	MEDIUM

R40. Gedragscodes of Certificeringsregelingen

R40. Gedragscodes of Certificeringsregelingen
Kwetsbaarheid
De verwerker beschikt niet over een goedgekeurde gedragscode of certificeringsregeling
Toelichting

R40. Gedragscodes of Certificeringsregelingen
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.
Maatregelen
Het contract met AWS voorziet standaard in de clausules voor het verwerkers contract. (https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/) Bijkomend geeft AWS aan dat: • De nodige maatregelen werden getroffen in de organisatie en het netwerk om de veiligheid en compliance met de AVG te respecteren • Een breach notification proces bestaat dat ervoor zorgt dat de verwerkingsverantwoordelijke geïnformeerd wordt over eventuele incidenten • De organisatie ISO 27001, 27017 en 27018 gecertificeerd is.
Residueel risico
Het residuele risico is eerder beperkt door de garanties die AWS voorziet, meer bepaald met zijn ISO 27001 certificatie. Doordat deze audit door een externe partij gebeurt kan objectief aangenomen worden dat de beschreven maatregelen ook effectief zijn toegepast.

Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

R41. Opleiding medewerkers

R41. Opleiding medewerkers
Kwetsbaarheid
De medewerkers zijn onvoldoende geïnformeerd over hoe om te gaan met de 'verwerking van persoonsgegevens'
Toelichting
-Hoewel de gegevens voor de contactopsporingsapplicatie gepseudonimiseerd zijn, zouden bepaalde Sciensano-medewerkers met toegangsrechten tot Gegevensbank I en VI acties inzake identificatie kunnen ondernemen. -In het kader van de covicodes hebben medewerkers van de callcenters van de betrokken administraties van de deelstaten net zoals voor manuele contactopsporing toegang tot nominatieve testresultaten van app-gebruikers die een dergelijke code willen aanvragen. Het betreft geen bijkomende toegang tot gegevens. Wat mogelijk wel een kwetsbaarheid kan zijn, is dat deze medewerkers ten onrechte covicodes aan een persoon ter beschikking stellen. Op dat moment zou ten onrechte TEK codes kunnen opgeladen worden
Maatregelen
-Alle betrokken medewerkers van Sciensano hebben een vertrouwelijkheids- en geheimhoudingsovereenkomst ondertekend. Via kwaliteitsdocumenten, business processen, workshops en het dagelijkse gebruik van security tools creëert de Sciensano dienst healthdata.be bewustzijn inzake het belang van vertrouwelijke omgang met gevoelige gegevens bij zijn medewerkers. Traces inzake toegang tot data zijn aanwezig. -De deelstaten en hun onderaannemers staan in voor opleidingen (o.a. over het correct interpreteren van data), verwerkersovereenkomsten en non-disclosure agreements met betrekking tot de call agent medewerkers die zij aantstellen.
Residueel risico

R41. Opleiding medewerkers	
Ondanks het creëren van bewustzijn, valt het niet 100% uit te sluiten dat bepaalde medewerkers al dan niet met slechte bedoelingen op een ongewenste manier met persoonsgegevens omgaat. Aangezien toegang tot de gegevens gelogd wordt, is er ontradend effect om gegevens onrechtmatig te gebruiken waardoor de probabiliteit verlaagd wordt.	
Risicoscore	
Probabiliteit na maatregelen	1
Impact na maatregelen	1
Risico	LAAG

Besluit

De Belgische contactopsporingsapplicatie oftewel de 'Coronalert App' maakt gebruik van het 3P-3T model dat gekenmerkt wordt door zijn hoge privacybescherming. Zo wordt er gewerkt met geheime sleutels die de identificatie van besmette personen vermijden. Risicovolle contacten kunnen door de gebruiker anoniem gemeld worden *(geen exacte tijd, geen plaats, geen identiteit)*. De gebruiker van de applicatie bepaalt zelf of hij de app installeert, gebruikt en of hij/zij gegevens wil uitwisselen. Gegevens worden slechts uitgewisseld met een centraal platform indien een besmette persoon daartoe zelf acties onderneemt en dus zijn instemming voor leent. In vergelijking met de bestaande gegevensverwerkingen voor manuele contactopsporing biedt de contactopsporingsapplicatie meer autonomie aan de burger en worden er minder gegevens verzameld.

De uitkomsten van de gegevensbeschermingseffectbeoordeling geven aan dat er werd rekening gehouden met aanbevelingen van het Europees Comité voor gegevensbescherming *voor het gebruik van locatiegegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19* zoals

- het vrijwillig gebruik van de app;
- geen gebruik van locatiegegevens;
- enkel gebruik van onpersoonlijke willekeurige ID's (die regelmatig vernieuwd worden);
- enkel gebruik voor het primaire doel (met name personen waarschuwen inzake besmettingsrisico's);
- tijdelijkheid van de applicatie en serverinfrastructuur (desactivatie na einde van crisisperiode);
- enkel verwerking van strikt noodzakelijke (gezondheids)gegevens;
- implementatie van afdoende technische en organisatorische maatregelen ter bescherming van de gegevens (o.a. gebruik van proxy-server, niet-colluderende servers) en
- bescherming tegen manipulatie (valse waarschuwingen over besmettingsrisico's) door kwaadwillige gebruikers.

Er is met andere woorden een duidelijk wettelijk kader dat de rechtsgrond definieert, de doelstellingen en data ontvangers beperkt, de korte bewaartermijnen van gegevens vastlegt alsook de minimale gegevens die verzameld mogen worden exhaustief opsomt (bestaande uit een Samenwerkingsakkoord en een Uitvoeringsakkoord). Dit wettelijk kader werd afgetoetst bij de Raad van State en de Gegevensbeschermingsautoriteit en op basis van hun feedback versterkt of verduidelijkt. Hoewel, de vernietiging van bepaalde delen van het wettelijke kader door lopende rechtsprocedures nog mogelijk zijn, kan er verwacht worden dat de wetgever, gelet op het maatschappelijke en politieke draagvlak om COVID-19 te bestrijden, eventuele gebreken (snel en/of retroactief) zal herstellen. De gegevensbeschermingseffectbeoordeling zal in dat geval ook

geactualiseerd worden. Naast het wettelijk kader is er de architectuur die aspecten als pseudonimisatie, geëncrypteerde data transfers, continuïteit van dienstverlening, privacy by default, verwijdering van gegevens en autorisaties voor waarschuwingen incorporeert.

Wijzigingen aan het wettelijk kader en/of de architectuur met een negatieve impact op de bescherming van de rechten en vrijheden van de betrokkenen lijken minder realistisch door de voorziene governance structuur voor het monitoren van de werking van de app en het belang dat gehecht wordt aan de openbare raadpleging over de contactopsporingsapplicatie (o.a. gericht op het vergroten van publiek vertrouwen in de app). De ontwikkeling van de app en bijhorende documentatie (bijvoorbeeld een ontwerp-privacyverklaring) gebeurt vanuit een multidisciplinaire benadering *(juridisch, app design, cybersecurity, epidemiologisch, …),* met consultatie van diverse stakeholders en met aandacht voor sociale bezorgdheden zoals e-inclusie en gebruiksvriendelijkheid. Het is met andere woorden geen geïsoleerd verhaal. Deze participatieve aanpak biedt naast de technische audit controle op de handhaving van privacybeschermende maatregelen.

Er zijn diverse maatregelen voorzien waardoor de residuele risico's inzake het niet respecteren van transparantie voor de betrokkenen, rechtmatigheid, dataminimalisatie, doelbinding, opslagbeperking en de bescherming van vertrouwelijkheid en veiligheid als laag of medium beschouwd kunnen worden. Daarbij dient aandacht besteed te worden aan verdere follow-up van bepaalde maatregelen zoals

- de evaluaties van de beschikbare communicatiekanalen en
- de uitkomsten van veiligheidsaudits die mogelijke acties vereisen.

Wat de rechten van de betrokkenen betreft, leidt de hoge graad van pseudonimisatie er toe dat rechten moeilijk kunnen worden uitgevoerd door de verwerkingsverantwoordelijke Sciensano. De moeilijkheid inzake identificatie van de betrokkene verhindert Sciensano bijvoorbeeld om aangevraagde correcties of bezwaren inzake verwerking van gegevens tot uitvoer te brengen. De impact op de betrokkene is evenwel beperkt omwille van bescherming van identiteit en de korte bewaartermijnen van gegevens binnen de serverinfrastructuur.

Uit de gegevensbeschermingseffectbeoordeling kwamen geen residuele risico's tot uiting die ook na de voorziene maatregelen nog als hoog gecategoriseerd werden. De gekende problematiek van het risico op vals-positieven bij COVID-19 labotesten verdient evenwel bijzondere aandacht. Een waarschuwing omtrent een risico-contact op basis van een vals-positief resultaat kan namelijk tot onnodige quarantaine leiden. Blijvende sensibilisatie van clinici inzake de detectie van vals-positieven en communicatie over vals-positieven ten aanzien van de bevolking is aangeraden om op die manier onterechte waarschuwingen beperkt te houden.

Gelet op

a) de hoge beleidsmatige, juridische en technische beschermingen voor de betrokkenen,
b) de ruime transparantie inzake architecturale documentatie (o.a. algoritme voor berekening blootstellingsrisico's, broncode, auditrapport)
c) het uitgebreide pakket aan risico-verminderende maatregelen,
d) de afwezigheid van hoge residuele risico's (enkel lage of medium risico's),
e) de maatschappelijke meerwaarde van de contactopsporingsapplicatie en
f) de inachtneming van "privacy by design and by default" door de EU Gateway dienst

geven de gegevensbeschermingsfunctionarissen van de betrokken overheidsdiensten *(Sciensano en de deelstatelijke gezondheidsadministraties)* een positief advies voor de gegevensverwerkingen die gepaard gaan met de Coronalert App.