

# JUSTEL - Geconsolideerde wetgeving

<http://www.ejustice.just.fgov.be/eli/besluit/2020/09/17/2020043045/justel>

---

Dossiernummer : 2020-09-17/02

## Titel

17 SEPTEMBER 2020. - Koninklijk besluit 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

Bron : SOCIALE ZEKERHEID

Publicatie : Belgisch Staatsblad van 17-09-2020 bladzijde : 66960

Inwerkingtreding : 18-09-2020

---

## Inhoudstafel

[HOOFDSTUK I.](#) - Definities

Art. 1

[HOOFDSTUK II.](#) - Algemeen

Art. 2

[HOOFDSTUK III.](#) - Technische specificaties en interoperabiliteit

Art. 3-4

[HOOFDSTUK IV.](#) - Informatieverplichting

Art. 5

[HOOFDSTUK V.](#) - Controle

Art. 6

[HOOFDSTUK VI.](#) - Inwerkingtreding

Art. 7-8

---

## Tekst

[HOOFDSTUK I.](#) - Definities

Artikel [1](#). Voor de toepassing van dit besluit wordt verstaan onder:

1° koninklijk besluit nr. 44: 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;

2° Gegevensbank I: de Gegevensbank I bedoeld in artikel 1, § 1, 5° van het koninklijk besluit nr. 44;

3° Gegevensbank V: de Gegevensbank V bedoeld in artikel 1, § 1, 9° van het koninklijk besluit nr. 44;

4° 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° ;

5° test: een coronavirus COVID-19 test waarmee wordt nagegaan of een persoon met het coronavirus COVID-19 besmet is;

6° app: de digitale contactopsporingsapplicatie CoronAlert, die door de gefedereerde entiteiten ter beschikking wordt gesteld;

7° 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;

8° 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, zoals de sterkte van het verzonden signaal;

9° 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;

10° risicocontact: een contact gedurende minstens vijftien minuten binnen een afstand van minder dan twee 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;

11° testnummer: willekeurige combinatie van enen en nullen, die wordt gebruikt om aan te tonen dat de beveiligde sleutels afkomstig zijn van een correcte app, met name een authentieke Coronalert app die geïnstalleerd is op de smartphone van de gebruiker op het moment dat hij/zij een test aanvraagt, zonder deze app te identificeren;

12° testcode: een code die bestaat uit willekeurige cijfers en wordt aangemaakt door de app bij de aanvraag van een test.

## HOOFDSTUK II. - Algemeen

Art. 2. § 1. Overeenkomstig artikel 14, § 1 van het koninklijk besluit nr. 44 biedt de app de volgende functionaliteiten aan en voert volgende verwerkingen uit:

1° Het registreren, op niet-gepersonaliseerde wijze, van de contacten van de gebruiker van de app met andere gebruikers van de app:

a) elke app genereert elke dag een andere beveiligde sleutel;

b) de beveiligde sleutel is enkel gekend op de smartphone waarop de app is geïnstalleerd;

c) op basis van de beveiligde sleutel worden niet-gepersonaliseerde tijdelijke serienummers gegenereerd;

d) op geregelde basis stuurt elke smartphone waarop de app is geïnstalleerd een niet-gepersonaliseerde tijdelijk serienummer uit als een Bluetooth baken; minstens om de twintig minuten wordt een ander niet-gepersonaliseerd tijdelijk serienummer uitgestuurd om te beletten dat deze niet-gepersonaliseerde tijdelijke serienummers kunnen gebruikt worden om een gebruiker te volgen; na de uitzendperiode wordt een niet-gepersonaliseerd tijdelijk serienummer niet bewaard op de smartphone die het serienummer verzonden heeft;

e) elke smartphone waarop de app is geïnstalleerd, slaat de Bluetooth bakens met de niet-gepersonaliseerde tijdelijke serienummers op die door andere smartphones op een beperkte afstand worden uitgezonden, samen met de dag waarop het baken is ontvangen en de signaalsterkte;

f) de niet-gepersonaliseerde tijdelijke serienummers worden bewaard op de ontvangende smartphone gedurende veertien dagen en daarna verwijderd.

2° Het aanmaken en overmaken van een testcode bij de aanvraag van een test:

a) in geval van symptomen van of risico op besmetting met het coronavirus COVID-19 wordt, in geval een gebruiker van de app zich laat testen, de datum vastgesteld waarop de gebruiker vermoedelijk besmettelijk is geworden; de app genereert een testnummer en berekent de testcode als een éénwegsfunctie van het testnummer en van de datum waarop de gebruiker besmettelijk is geworden;

b) de testcode wordt op initiatief van de gebruiker samen met het identificatienummer van de sociale zekerheid (INSZ) elektronisch aan Sciensano doorgegeven hetzij door de arts die de test voorschrijft, via een softwarepakket, hetzij door de patiënt via een webtoepassing en samen met de datum van de staalafname en de datum waarop de gebruiker besmettelijk is geworden, opgeslagen in Gegevensbank I;

3° Het opvragen van een resultaat van de test:

a) als een resultaat van een test of een ernstig vermoeden van besmetting met het coronavirus COVID-19 beschikbaar is in Gegevensbank I, worden de testcode, de datum van staalafname en de datum waarop de gebruiker besmettelijk is geworden, door Gegevensbank I meegedeeld aan de Gegevensbank VI; na bevestiging van ontvangst van deze gegevens door Gegevensbank VI, wordt de testcode automatisch verwijderd uit Gegevensbank I, waardoor geen connectie meer mogelijk is tussen de gegevens in Gegevensbank I en de gegevens van de app;

b) de app contacteert op geregelde tijdstippen de Gegevensbank VI om na te gaan of er al een resultaat van een test of een ernstig vermoeden van besmetting met het coronavirus COVID-19 beschikbaar is voor de combinatie testcode en datum waarop de gebruiker besmettelijk is geworden; de app kan dus het resultaat van

een test bekomen zonder dat de gebruiker geïdentificeerd moet worden;

c) na bevestiging van ontvangst van het resultaat van een test door de app worden het resultaat van de test en de bijhorende testcodes en data verwijderd uit Gegevensbank VI; 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;

d) het testresultaat wordt ten laatste vierentwintig uur na het tonen van het resultaat aan de gebruiker uit de app verwijderd;

e) als de app veertien dagen na de datum van het aanmaken van de testcode nog geen resultaat van de test heeft ontvangen, worden het testnummer, de testcode en de datum waarop de gebruiker besmettelijk is geworden uit de app verwijderd;

4° het doorsturen van de beveiligde sleutels naar Gegevensbank V in geval van een positief resultaat van een test

a) na ontvangst van een positief resultaat van een test kan de gebruiker toestemming geven om de beveiligde sleutels, het testnummer en de datum waarop hij besmettelijk is geworden, op te laden in Gegevensbank V;

b) de app verzamelt geen locatiegegevens; de gebruiker kan echter wel binnen de app vrijwillig aangeven in welk(e) land(en) hij op een bepaalde datum is geweest om te kunnen samenwerken met de contactopsporingsapplicaties van andere landen; desgevallend worden de beveiligde sleutels naar het door de gebruiker aangegeven land gestuurd;

c) na bevestiging van ontvangst door Gegevensbank V van de gegevens vermeld onder a) en b), worden het resultaat van de test, de beveiligde sleutels, de lijst van landen, het testnummer, de testcode, en de datum waarop de gebruiker besmettelijk is geworden uit de app verwijderd;

d) op geregelde tijdstippen genereert Gegevensbank V uit de gegevens vermeld onder 4° a) het testnummer en gaat ze na of er een geldige autorisatiecode bestaat voor elke testcode en datum; als aan alle voorwaarden voldaan is, worden de beveiligde sleutels opgenomen in Gegevensbank V;

e) de beveiligde sleutels worden veertien dagen na de datum van ontvangst uit Gegevensbank V verwijderd;

5° Het opsporen van contacten:

a) de app contacteert op geregelde tijdstippen Gegevensbank V en downloadt de sleutels en de bijhorende besmettelijke dagen van alle besmette gebruikers; deze lijst wordt digitaal gedagtekend zodat de app de authenticiteit van deze lijst kan nagaan aan de hand van de publieke sleutel van Gegevensbank V;

b) de app ontcijfert met deze beveiligde sleutels de door deze sleutels gegenereerde niet-gepersonaliseerde tijdelijke serienummers en gaat na of deze serienummers ook opgeslagen zijn in de app; de app berekent op basis van het verschil van de sterkte tussen het verzonden en ontvangen signaal de signaalverzwakking en schat de afstand van het contact in; de totale duur van mogelijke contacten wordt berekend op basis van het aantal serienummers dat overeenkomt; op deze manier kan de app nagaan of in de voorbije veertien dagen een risicocontact heeft plaatsgevonden;

c) als de app een risicocontact detecteert, informeert de app de gebruiker over een mogelijk risico op besmetting met het coronavirus COVID-19.

§ 2. De app laadt op geregelde basis dummy sleutels op in Gegevensbank V. Voor zij dat doet stuurt de app een aantal dummy verzoeken naar Gegevensbank VI, die dummy antwoorden terugstuurt. De dummy sleutels hebben geen geldige autorisatiecode en worden dus niet opgenomen in Gegevensbank V. Op deze manier kan men besmette gebruikers niet onderscheiden van niet-geteste of niet-besmette gebruikers op basis van de communicatiepatronen van de app.

Als er minder dan tien beveiligde sleutels zijn opgeladen op één dag, worden in Gegevensbank V bijkomende dummy beveiligde sleutels opgeladen tot het totaal van tien bereikt wordt.

### HOOFDSTUK III. - Technische specificaties en interoperabiliteit

Art. 3. De app wordt aangeboden op iOS en Android.

Art. 4. § 1. De app moet :

1° eenvoudig te installeren en te gebruiken zijn;

2° werken met een beperkt batterijverbruik;

3° voldoende nauwkeurig zijn; dit betekent dat de app enkel contacten van minstens vijftien minuten binnen een afstand van minder dan twee meter als risicocontact detecteert;

4° internationale interoperabiliteit ondersteunen en het Bluetooth-gedeelte van de app in een zo groot aantal mogelijk landen bruikbaar maken door dit gedeelte compatibel te maken met de apps gebruikt in de meeste EU landen.

§ 2. De Gegevensbank V en de Gegevensbank VI, en de daarvoor gebruikte infrastructuur moet:

1° een goede performantie leveren, schaalbaar zijn voor gebruik door meerdere miljoenen gebruikers en bestand zijn tegen aanvallen;

2° de mogelijkheid bieden om de beveiligde sleutels uit te wisselen met andere landen binnen de EU en dit rechtstreeks of via de EU Federation Gateway Service; beveiligde sleutels worden enkel verstuurd naar de tegenhanger van Gegevensbank V van dat land of regio als:

a) dat land of regio een gedecentraliseerde contactopsporingsapp heeft, erkend door de nationale of regionale gezondheidsdienst met een Bluetooth gedeelte dat compatibel is met de Belgische app;

b) er voldoende waarborgen zijn voor de gegevensbescherming met inbegrip van de veilige communicatie tussen Gegevensbank V en haar tegenhanger;

c) de gebruiker van de app heeft aangegeven dat hij/zij dat land of die regio bezocht heeft in de periode waarin

hij/zij besmettelijk was. Voor het ontvangen van beveiligde sleutels uit andere landen of regio's gelden voorwaarden a) en b);

d) de beveiligde sleutel van het buitenland afkomstig is van een gebruiker die aangegeven heeft dat hij/zij België bezocht heeft in de periode waarin hij/zij besmettelijk was. Nadat de beveiligde sleutels zijn aangekomen in Gegevensbank V of in de tegenhanger ervan in een ander land of regio, worden ze gedownload in de apps van het land of de regio.

3° valse of incorrecte rapportering van besmettingen vermijden; de rapportering van een besmetting kan enkel na een positief resultaat van een test of na een vaststelling door een arts van een ernstig vermoeden dat een persoon besmet is met het coronavirus COVID-19;

4° dermate zijn opgezet dat er geen relatie kan gelegd worden tussen berichten, zoals beveiligde sleutels en testresultaten en IP-adressen van gebruikers.

§ 3. De app en de serverinfrastructuur moeten de persoonlijke levenssfeer van de gebruikers waarborgen, gebaseerd zijn op minimale gegevensverwerking en gegevensbescherming door ontwerp. Dit houdt onder meer in dat:

1° er geen locatie-informatie mag ingezameld worden;

2° alle communicatie tussen de app en de gegevensbanken versleuteld wordt;

3° er geen informatie wordt verwerkt over wie waar door wie besmet is;

4° er geen beveiligde sleutels worden verzameld van een gebruiker die niet besmet is;

5° het systeem uitgeschakeld kan worden en alle opgeslagen informatie verwijderd kan worden ten laatste vijf dagen na de publicatie van het koninklijk besluit dat het einde van de toestand van de coronavirus COVID-19 epidemie afkondigt;

6° bij uitwisseling van gegevens naar Gegevensbanken I en V en naar de Gegevensbank VI slechts het minimum aan gegevens mag uitgewisseld worden om het resultaat van de test te kunnen sturen naar de juiste app, zodat de kans op identificatie van de betrokkene minimaal gehouden wordt;

7° het niet mogelijk is om het systeem of de gegevens voor andere doeleinden te gebruiken.

§ 4. De werking van het systeem voorziet in minimale administratieve lasten middels een eenvoudige ingave van de testcode bij het aanvragen van een test.

#### HOOFDSTUK IV. - Informatieverplichting

Art. 5. § 1. De gebruikers worden, bij de installatie en voor het gebruik ervan, geïnformeerd over de werking van de app en de interactie ervan met de Gegevensbanken I, V en VI.

Hiertoe wordt op de website [www.coronalert.be](http://www.coronalert.be) alle nuttige informatie over de app en de gegevensbanken gepubliceerd, onder meer de functionaliteiten, de werking, het charter, de privacyverklaring en de gegevensbeschermingseffectbeoordeling. De app zelf bevat ook verwijzingen naar informatie over de functionaliteiten, de werking en de privacyverklaring.

§ 2. De broncode van de app en van de programma's voor het beheer van de Gegevensbank V en de Gegevensbank VI in het bijzonder de onderdelen die de gegevens voor een test genereren, de resultaten van een test downloaden, de beveiligde sleutels opladen en het risico berekenen, evenals de gebruikersinterface van de app, worden aan de hand van een link publiek gemaakt op de website, bedoeld in § 1, eerste lid.

#### HOOFDSTUK V. - Controle

Art. 6. De werking en de noodzaak van de app wordt regelmatig gemonitord, geëvalueerd en bijgesteld onder aansturing van het Interfederaal Comité Testing en Tracing, bestaande uit vertegenwoordigers van de gefedereerde entiteiten, Sciensano, het eHealth-platform en twee wetenschappelijke experts. Dit comité kan ondersteund worden door een interdisciplinaire werkgroep van wetenschappelijke experts.

De app zal tevens het voorwerp uitmaken van een informatieveiligheidsaudit door een instantie onafhankelijk van diegene die de app ontwikkeld heeft, waarbij onder meer wordt nagegaan of deze beantwoordt aan de informatieveiligheidsvoorwaarden en in overeenstemming is met de geldende regelgeving.

#### HOOFDSTUK VI. - Inwerkingtreding

Art. 7. Dit besluit treedt in werking op 18 september 2020.

Art. 8. De minister van Sociale Zaken en Volksgezondheid is belast met de uitvoering van dit besluit.