Ministerie van Volksgezondheid,
Welzijn en Sport

> Retouradres Postbus 20350 2500 EJ Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34
www.rijksoverheid.nl

Ons kenmerk
3233345-1013153-DICIO

Bijlagen
1

Uw brief
20 juli 2021

Correspondentie uitsluitend richten aan het retouradres met vermelding van de datum en het kenmerk van deze brief.

Datum 24 augustus 2021
Betreft Antwoorden op Kamervragen over Incident Testcoronanu BV en de ernstige tekortkoming in de informatiebeveiliging

Geachte voorzitter,

Hierbij zend ik u, mede namens de ministers van Justitie & Veiligheid en Infrastructuur & Waterstaat, de antwoorden op de vragen van de leden Rajkowski en De Vries (VVD) over het incident Testcoronanu BV en de ernstige tekortkoming in de informatiebeveiliging (2021Z13898).

Hoogachtend,

de minister van Volksgezondheid,
Welzijn en Sport,

Hugo de Jonge

Antwoorden op Kamervragen van de leden Rajkowski en De Vries (VVD) over het incident Testcoronanu BV en de ernstige tekortkoming in de informatiebeveiliging (ingezonden 20 juli 2021) (2021Z13898).

1. Hoeveel mensen zijn de dupe geworden van dit datalek als het gaat om de gevolgen voor hun vakantieplannen? Welke alternatieve mogelijkheden worden de getroffen mensen pro-actief geboden om een test voor reizen te kunnen krijgen om toch tijdig gereed te zijn voor hun vakantie c.q. reis? Hoe is of wordt hierover gecommuniceerd met de betrokken mensen?

Testaanbieder Testcoronanu BV heeft aangegeven dat op het moment van het incident 17.638 mensen nog een testafspraak hadden staan. Ik heb Testcoronanu BV verzocht om mensen die al wel getest waren en op korte termijn reizen hun testuitslag op een veilige andere wijze (bijvoorbeeld op papier) te verstrekken. Daarnaast is Testcoronanu BV verzocht om alle personen die nog een testafspraak hadden staan persoonlijk te informeren en door te verwijzen naar andere testaanbieders via het afsprakenportaal. Reeds uitgegeven QR-codes bleven geldig.

2. Klopt het dat in de brief te lezen is dat de testaanbieder verantwoordelijk is te onderzoeken of anderen dan de RTL-journalist zich toegang hebben verschaft tot de database? Gaat u erop toezien dat dit onderzoek degelijk wordt uitgevoerd en dat de bevindingen met u gedeeld worden?

Dit klopt. Het ministerie van VWS maakt het voor testaanbieders mogelijk om aan te sluiten op CoronaCheck en beoordeelt deze aanvragen. In dat kader doet het ministerie onderzoek naar de juistheid van de aangeleverde bewijsstukken door Testcoronanu BV. Testcoronanu BV is zelf verantwoordelijk voor de veiligheid van hun systemen en persoonsgegevens. De testaanbieder heeft aangegeven een extern onderzoeksbureau te hebben inegschakeld om dit incident nader te onderzoeken. Ik heb van de testaanbieder begrepen dat hierbij ook wordt nagegaan of anderen, naast de RTL-journalist, zich toegang hebben verschaft tot de betreffende database. In het kader van stelselbewaking (zie ook artikel 14 van de aansluitvoorwaarden) heb ik Testcoronanu BV gevraagd om de uitkomsten van dit onderzoek, zodra dit kan, ook met mij te delen.

3. Deelt u de mening dat het wenselijk is te weten hoeveel mensen uiteindelijk misbruik hebben gemaakt van dit lek en negatieve testbewijzen hebben gegenereerd? Wat gaat u met deze informatie doen? In hoeverre kunnen deze onterecht verkregen negatieve testbewijzen alsnog worden ingetrokken?

Deze mening deel ik. De testaanbieder doet hier nu nader onderzoek. Zie hiervoor ook het antwoord op vraag 2.

4. Klopt het dat in de database gegevens van 60.000 mensen te vinden waren inclusief hun volledige namen, woonadressen, e-mailadressen, telefoonnummers, Burgerservicenummers, paspoortnummers en medische gegevens? Zijn er indicaties dat deze gegevens door criminelen zijn buitgemaakt? Zo ja, wat gaat u doen om te voorkomen dat deze mensen slachtoffer worden van bijvoorbeeld phising of identiteitsfraude?

De testaanbieder heeft aangegeven dat vanaf het moment van aansluiten tot zaterdag 17 juli de gegevens van in totaal 60.541 personen in de betreffende database hebben gestaan. De database in kwestie werd, aldus de testaanbieder echter periodiek opgeschoond en daarom wordt dit aantal door de testaanbieder als bovengrens gehanteerd. Er hebben ons geen signalen bereikt dat anderen dan

de RTL-journalist zich toegang hebben verschaft tot de database teneinde gegevens in te zien of te wijzigen. Zoals ook in de beantwoording op vraag 2 is aangegeven, doet de testaanbieder hier momenteel nader onderzoek naar.

5. De Begeleidingscommissie Digitale Ondersteuning Bestrijding Covid-19 heeft in februari en april van dit jaar geadviseerd over privacybescherming en een toelatingskader voor apps met vaccinatie en/of testbewijzen, wat is er met deze adviezen gedaan?

In de stand van zaken covid-19 brief van 23 februari jl. ben ik nader ingegaan op het advies van de Begeleidingscommissie Digitale Ondersteuning Covid-19 over het toelatingskader voor apps met vaccinatie- en/of testbewijzen.[1] Dit advies zag op applicaties van derden en is nog niet aan de orde geweest omdat ik mijn aandacht vooralsnog richt op door de overheid gerealiseerde toepassingen voor zowel digitale als niet digitale test-, vaccinatie- en herstelbewijzen, in dit geval CoronaCheck. De adviezen gegeven in april jl. met betrekking tot het Europees Digitaal Covid Certificaat (DCC) zijn meegenomen in de uitwerking van het DCC. Hierover heb ik uw Kamer in de stand van zaken covid-19 brief van 28 mei jl. geïnformeerd.[2]

6. Klopt het dat in de brief is te lezen dat elke testaanbieder na aansluiting periodiek en actief wordt gemonitord? Wat is het verschil tussen monitoring, actieve en periodieke monitoring en hoe dragen deze verschillende soorten monitoring bij aan de veiligheidswaarborgen?

Het ministerie van VWS stelt aan testaanbieders die aangesloten willen worden op CoronaCheck strenge aansluitvoorwaarden. Deze voorwaarden zijn ook openbaar in te zien via Rijksoverheid.nl.[3] Na aansluiting is de testaanbieder zelf verantwoordelijk voor het loggen en monitoren van hun systeem. Het ministerie van VWS monitort in het kader van stelselcontrole of aangesloten testaanbieders de aansluitvoorwaarden naleven en met pentesten of er kwetsbaarheden zijn die moeten worden opgelost. Bevindingen uit deze monitoring worden met de testaanbieders gedeeld zodat zij deze kunnen oplossen. Indien nodig kan in voorkomende gevallen tot afsluiting worden over gegaan zoals bij Testcoronanu BV het geval is geweest.

7. In de brief is te lezen dat testaanbieders een pentestrapportage moeten overhandigen, welke eisen worden gesteld aan de pentest? Wat wordt de testaanbieder geacht te doen met de uitkomsten van de pentest en hoe ziet u hierop toe?

Testaanbieders moeten ervoor zorgdragen dat de aansluiting op CoronaCheck op een wijze is beveiligd die in overeenstemming is met geldende wet- en regelgeving, waaronder in het bijzonder de AVG en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Als onderdeel van de aansluitprocedure wordt gevraagd om ter ondersteuning hiervan bewijsstukken aan te leveren die onder meer bestaan uit een DPIA en een pentestrapportage. De eisen aan de pentestrapportage staan in artikel 9 van de eisen voor informatiebeveiliging en privacybescherming.[4]

---

[1] Kamerstuk 25 295, nr. 995
[2] Kamerstuk 25 295, nr. 1241
[3] https://www.rijksoverheid.nl/onderwerpen/coronavirus-covid-19/coronabewijs/coronacheck-voor-aanbieders-testen
[4] https://www.rijksoverheid.nl/documenten/publicaties/2021/04/29/eisen-informatiebeveiliging-en-privacybescherming

De pentesten moeten opgesteld zijn aan de hand van de internationale standaard Penetration Execution Standard (PTES). De aangeleverde pentestrapportage mag geen openstaande bevindingen met een CVSS-score (Common Vulnerability Scoring System) van 4,0 of hoger bevatten. Gevonden risicovolle bevindingen moeten zijn opgelost en er moet een hertest hebben plaatsgevonden. Naast de door de testaanbieder aan te leveren pentestrapportage wordt in de aansluitprocedure nu ook door het ministerie van VWS een extra controle ter verificatie van de pentest uitgevoerd. Ook hiervoor geldt dat bevindingen opgelost moeten zijn voordat kan worden overgegaan op formele aansluiting van de testaanbieder op CoronaCheck.

Zoals ik in mijn antwoord op vraag 2 aangeef, loopt er een onderzoek vanuit het ministerie naar de juistheid van de aangeleverde bewijsstukken door Testcoronanu BV.

8. Softwarecode is doorgaans aan verandering onderhevig, welke criteria stelt u aan het opnieuw uitvoeren van een pentest na het wijzigen van de softwarecode?

Bij substantiële wijzigingen van bijvoorbeeld de softwarecode moet dit door de aangesloten testaanbieders aan VWS gemeld worden. Er wordt vervolgens nagegaan in welke gevallen een nieuwe beoordeling, en dan ook een nieuwe pentest, voor de aansluiting op CoronaCheck noodzakelijk is.

9. Heeft Testcoronanu gebruik gemaakt van externe mensen of partijen bij het maken van hun digitale product? Zo ja, zijn deze mensen of partijen ook betrokken bij andere digitale overheidsoplossingen en deelt u de mening dat die andere oplossingen gecontroleerd moeten worden op privacy, veiligheid en betrouwbaarheid?

De testaanbieder heeft aangegeven dat er sprake is van een of meerdere externe dienstverleners die betrokken zijn geweest bij de ontwikkeling. Ik heb geen zicht op de opdrachtenportefeuille van deze dienstverleners.

10. Worden de bewijsstukken van alle aanbieders onderzocht, voordat tot aansluiting wordt overgegaan? Zo ja, hoe worden de bewijsstukken gecontroleerd en beoordeeld?

Testaanbieders moeten ter aansluiting op CoronaCheck voldoen aan een uitgebreide set aansluitvoorwaarden met betrekking tot technische vereisten en informatiebeveiliging. Deze zijn openbaar en te vinden via de website van de Rijksoverheid.[1] De aansluitvoorwaarden vormen een juridische overeenkomst tussen de Staat der Nederlanden (het ministerie van VWS) en de testaanbieder bij de aansluiting op de app. Hieruit moet blijken dat voldaan wordt aan wet- en regelgeving én aan de geldende normen voor informatiebeveiliging in de zorg (waaronder NEN7510, 7512, 7513). De aansluiting vindt via een aantal stappen plaats waarbij er ook naar bewijsstukken zoals een DPIA en pentestrapportage wordt gevraagd. Deze stukken worden met behulp van een beoordelingssjabloon (zie ook bijlage) gecontroleerd en beoordeeld aan de hand van de aansluitvoorwaarden. Pas na volledige beoordeling hiervan en mits er geen risicovolle bevindingen meer zijn geconstateerd kan worden overgegaan op formele aansluiting van de testaanbieder op CoronaCheck.

11. Klopt het dat Testcoronanu een (tweede data)lek heeft veroorzaakt door alle emailadressen van de mensen waarvan hun coronatest werd geannuleerd, in de CC te zetten? Hoe beoordeelt u dit?

Net als u ben ik bekend met de berichtgeving hierover. In het algemeen moet met persoonsgegevens zeer zorgvuldig worden omgegaan, in het bijzonder met medische persoonsgegevens. Het is in deze aan de Autoriteit Persoonsgegevens om hierop toe te zien.

12. Bent u bereid de bevindingen van hun onderzoek naar de aangeleverde stukken, zoals een Data Protection Impact Assessment (DPIA) en pentestrapportage met de Tweede Kamer te delen? Zo nee, waarom niet? Zo ja, wanneer kan de Kamer deze verwachten?

Het ministerie van VWS heeft nader onderzoek gestart naar de juistheid van de aangeleverde bewijsstukken. Indien deze bevindingen aanleiding geven om de aansluitvoorwaarden aan te passen zal ik deze uiteraard met uw Kamer delen. Ik kan echter niet toezeggen dat ook de door de testaanbieder aangeleverde DPIA's en pentestrapportages met uw Kamer worden gedeeld. Conform de aansluitvoorwaarden zijn zij zelf verwerkingsverantwoordelijke in het kader van de AVG en voeren eigenstandig een DPIA en beveiligingsonderzoeken uit.