



Gegevensbeschermingseffectbeoordeling (DPIA)

VWS | Directie Informatiebeleid / CIO
DPIA COVID-19 notificatie-app

Maatregelen
nemen
Privacybewustwording
Doelbinding
PIA
Noodzaak
Effecten in kaart
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond.
Met open vizier

Vaststelling VWS

Den Haag, 7 juli 2020

Ministerie van Volksgezondheid, Welzijn en Sport

Voor deze de gemandateerd opdrachtgever,

Sylvia Bronmans | Programmadirecteur, Realisatie Digitale Ondersteuning

Documenten:

DPIA

Advies FG

Reactie FG op advies FG

Advies van de Functionaris voor Gegevensbescherming

Den Haag, 7 juli 2020

Henriëtte Westerling - Woltman

Zie Advies FG als bijlage bij de DPIA

Gegevensbeschermingseffectbeoordeling (DPIA)

















VWS | Directie Informatiebeleid / CIO
DPIA COVID-19 notificatie-app

Contact:

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

Versie: 1 juli 2020

Inhoudsopgave

Inleiding & definities	6
A. Beschrijving kenmerken gegevensverwerkingen	8
1. Voorstel 	8
2. Persoonsgegevens 	11
3. Gegevensverwerkingen 	13
4. Verwerkingsdoeleinden 	15
5. Betrokken partijen 	15
7. Verwerkingslocaties 	18
8. Techniek en methode van gegevensverwerking 	19
9. Juridisch en beleidsmatig kader 	21
10. Bewaartermijnen 	21
B. Beoordeling rechtmatigheid gegevensverwerkingen	23
11. Rechtsgrond 	23
12. Bijzondere persoonsgegevens 	25
13. Doelbinding 	25
14. Noodzaak en evenredigheid 	25
15. Rechten van de betrokkene 	30
C. Beschrijving en beoordeling risico's voor de betrokkenen	31
16. Risico's 	31
D. Beschrijving voorgenomen maatregelen	31
17. Maatregelen 	31
Bijlage 1: Risico's en Maatregelen	38
1. Gebruiker onvoldoende specifiek geïnformeerd	39
2. Onvrijwillige installatie	40
3. Geblokkeerde app in de store	41
4. Replay van RPI's	42
5. Gemanipuleerde RPI's via relay	43
6. Denial of Service	44
7. Onbevoegde tracking	45
8. Reconstructie van gangen van mobiele telefoons	46
9. Depseudonimisatie	47
10. Justitie of inlichtingendiensten verschaffen zich toegang tot telefoon	48
11. API of andere apps slaan RPI's te lang op	49
12. Derden slaan RPI's te lang op	50
13. Besturingssysteem of andere apps zien TEKs	51
14. Wetenschappers verzamelen TEKs	52
15. Menselijke fouten bij vrijgeven code	53
16. Gebruiker drukt op upload knop zonder besmetting	54
17. Gebruiker onvoldoende specifiek geïnformeerd	55

18.	Upload onder druk.....	56
19.	Backend niet beschikbaar.....	57
20.	Collission TEKs.....	59
21.	Nep-backend.....	60
22.	Backend op netwerk geblokkeerd.....	61
23.	Datalekken.....	62
24.	Toegang door OM/Politie of inlichtingendiensten.....	63
25.	Belastingdienst verschaft toegang tot TEKs.....	64
26.	Verkeersanalyse.....	65
27.	Derden bewaren TEKs te lang.....	66
28.	Derden analyseren publieke TEKs.....	67
29.	Herintroductie oude TEKs.....	68
30.	App raakt corrupt.....	69
31.	Screenshot notificatie.....	70
32.	Omkeerbaarheid RPI's of TEKs.....	71

Inleiding & definities

Aanleiding

In de huidige fase van de bestrijding van de epidemie van het Covid-19, waarin het aantal nieuwe besmettingen, ziekenhuisopnames en nieuwe opnames op de IC-afdelingen is afgenomen, is Nederland in een overgangsfase terechtgekomen waarin beperkende maatregelen worden versoepeld en het aantal contacten tussen personen geleidelijk weer toeneemt. Deze versoepelingen vergen een slimme controle-strategie bestaande uit een combinatie van begeleidende maatregelen en de medewerking van de gehele bevolking.

Het Outbreak Management Team (hierna: OMT) heeft geadviseerd om met het oog op het intensievere testbeleid de mogelijkheden voor ondersteuning van bron- en contactopsporing met behulp van mobiele applicaties te onderzoeken.¹ Ook de Tweede Kamer heeft in de breed aangenomen motie Jetten c.s. overwogen dat het gebruik van apps kan bijdragen aan het beheersen van het virus.² De inzet van dergelijke apps heeft ook de aandacht van andere Europese lidstaten en de Europese Commissie.³

Na de uitbraak van COVID-19 (hierna: het virus) werd duidelijk dat bij het oplaaien van het virus onder de bevolking het bron- en contactonderzoek kan worden versneld door zicht te krijgen op potentiële zieken door ze middels een digitale weg te waarschuwen.

In de kamerbrieven van respectievelijk 6 en 19 mei 2020 heeft de minister van Volksgezondheid, Welzijn en Sport (hierna: VWS) een zogenaamde corona-app voor het door de gemeentelijke gezondheidsdiensten (hierna: GGD-en) uit te voeren bron- en contactonderzoek van COVID-19-infecties aangekondigd. Inmiddels wordt deze app aangeduid als de notificatie app (hierna ook: de app).

Dit document bevat de gegevensbeschermingseffectbeoordeling (GEB, in het Engels: Data Protection Impact Assessment, hierna: DPIA) van deze voorgenomen app conform artikel 35 van de Algemene Verordening Gegevensbescherming (hierna: AVG).

Gebruikte afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
BLE	Bluetooth Low Energy
DPIA	Data Protection Impact Assessment

¹ Bijlage 929506 bij *Kamerstukken II 2019/20, 25 295*, nr. 219.

² *Kamerstukken II 2019/20, 25 295*, nr. 223.

³ https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

D3P-T	Decentraliced, Privacy-Preserving Proximity Tracing
EDPB	European Data Protection Board
EHRM	Europees Hof van de Rechten van de Mens
GGD	Gemeentelijke Gezondheidsdienst
HvJ	Hof van Justitie van de Europese Unie
RPI	Rolling Proximity Indicator
UAVG	Uitvoeringswet AVG
TEK	Temporary Exposure Key, in de relevante Google en Apple documentatie worden deze aangeduid als Diagnosis Key op het moment als iemand als geïnfecteerd is aangemerkt.
VWS	Het ministerie van Volksgezondheid, Welzijn en Sport
Wpg	Wet publieke gezondheid
WP29	Article 29 Working Party, de voorganger van de EDPB die zijn mandaat aan art. 29 van Richtlijn 95/46/EG ontleende.

A. Beschrijving kenmerken gegevensverwerkingen

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

Onder A wordt de eerste stap beschreven van de DPIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel



Beschrijf het voorstel waar de DPIA op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

De voorgestelde verwerking van persoonsgegevens vindt plaats in een notificatie-app. Doel daarvan is om in aanvulling op het bestaande bron- en contactonderzoek van de GGD-en bij een geconstateerde COVID-19 infectie andere gebruikers van de app die in de nabijheid van de geïnfecteerde zijn geweest te informeren over de verhoogde kans op een besmetting met COVID-19 en een advies om contact op te nemen met de GGD in hun regio.

Bij deze notificatie-app wordt gebruik gemaakt van een implementatie van het zogenaamde Decentralized Privacy-Preserving Proximity Tracing (DP3T protocol)⁴ zoals dat is geïntegreerd in de besturingssystemen van Apple (iOS) en Google (Android).⁵

Het gebruik van de notificatie-app doorloopt in de tijd de volgende fasen:

- Installatiefase
- Uitwisselingsfase
- Validatiefase
- Koppelingsfase
- Notificatiefase

Installatiefase

In deze fase downloadt de burger, de gebruiker, de app van de app store van Google (in het geval van een smartphone met Android als besturingssysteem) of Apple (in het

⁴ DP3T wordt omschreven als "a secure, decentralized, privacy-preserving proximity tracing system. Its goal is to simplify and accelerate the process of identifying people who have been in contact with an infected person, thus providing a technological foundation to help slow the spread of the SARS-CoV-2 virus. The system aims to minimise privacy and security risks for individuals and communities and guarantee the highest level of data protection." Voor deze DPIA is uitgegaan van het Whitepaper Decentralized Privacy-Preserving Proximity Tracing Version: 25 May 2020. Dit document is, met de overige documentatie over DP3T, te vinden in het DP3T Repository op <https://github.com/DP-3T/documents> (laatst. geraadpl. 1 juli 2020).

⁵ De documentatie over de door Apple en Google ontwikkelde API's is te vinden via www.apple.com/covid19/contacttracing (laatst. geraadpl. 1 juli 2020); Exposure Notification. FAQ, v1.1 May 2020; Exposure Notification. Cryptography Specification, v1.2 April 2020; Exposure Notification. Bluetooth Specification, v1.2, April 2020.

geval van een smartphone met iOS als besturingssysteem) en installeert deze op zijn of haar smartphone.

Uitwisselingsfase

In deze fase worden pseudonieme identificatiesleutels, Rolling Proximity Indicators (hierna: RPIs of RPIs/contactcodes), uitgewisseld tussen smartphones van gebruikers van de app door middel van Bluetooth. Deze RPIs zijn gegenereerd op basis van zogenaamde Temporary Exposure Keys (TEKs) en hebben een geldigheidsduur van tien tot twintig minuten. De TEKs en RPIs worden elke dag opnieuw gegenereerd en zijn volledig willekeurige (cryptografisch random). Zowel de TEKs als de RPIs zijn gepseudonimiseerde identificatiesleutels.⁶

De software waarmee de TEKs en RPIs/contactcodes worden gegenereerd is compatible met de Exposure Notification Application Programming Interface (API) die ten behoeve van contact tracing is ontwikkeld door Apple en Google. In de uitwisselingsfase worden gegevens meegestuurd die van belang zijn voor een toekomstige inschatting van een infectierisico, zijnde: de sterkte van het Bluetooth-sigitaal en de duur van de uitwisseling. De RPIs/contactcodes en eigen TEKs worden veertien dagen bewaard op de smartphone van de gebruikers.

Validatiefase

Wanneer door de GGD is geconstateerd dat een gebruiker is geïnfecteerd kan deze gebruiker ervoor kiezen om de eigen TEKs, tezamen met een unieke autorisatiecode, naar de back-end-server te sturen. De autorisatiecode wordt door de gebruiker zelf gegenereerd met behulp van een in de app aangeboden functionaliteit. Om deze code te valideren verzoekt de GGD de gebruiker om naar een bepaald scherm in de app te gaan en een code van zes posities op te lezen. De GGD plaatst deze code, met de datum van de eerste ziekte dag, in het zgn. GGD-portaal van de app, welk portaal alleen toegankelijk is voor GGD-medewerkers met een zgn. GGD Identity Hub account, dat o.a. voorziet in 2-factor authenticatie.

De back-end server accepteert alleen TEKs van gebruikers als daarbij een autorisatiecode wordt aangeboden die op deze wijze door de GGD is gevalideerd. Op de server worden dus alleen TEKs vastgelegd, nadat de back-end-server in de GGD-portaal een autorisatiecode heeft aangetroffen die overeenkomt met de autorisatiecode die de gebruiker zelf met de TEKs naar de back-end-server heeft gestuurd.

Op de back-end-server worden de TEKs geconverteerd naar Diagnosis Keys (DKs). Ook wordt voor elke DK de datum van de eerste ziekte dag vergeleken met de datum van de TEKs. Op basis daarvan wordt door de server een zgn. TransmissionRiskValue (high, mid, low) bepaald.

De back-end server stelt de DKs vervolgens beschikbaar, zodat deze kunnen worden opgehaald door de smartphones van andere gebruikers waarop de app is geïnstalleerd.

⁶ Zie voor een nadere (technische) uiteenzetting: Exposure Notification. Cryptography Specification, v1.2 April 2020, te vinden via www.apple.com/covid19/contacttracing (laatst. geraadpl. 1 juli 2020).

In aanvulling op de DKs, eerste ziektedag en autorisatiecode wordt er in deze fase ook het IP-adres van de smartphone van de gebruiker meegestuurd naar de back-end server -- dit is inherent aan het gebruik van internet en IP-technologie. Op de server wordt dit IP-adres evenwel gesepareerd, zodat er op de server geen IP-adressen van gebruikers worden vastgelegd en niet kan worden herleid wie welke informatie heeft verstuurd (zie voor meer informatie hierover onderdeel 3, subonderdeel 'Validatiefase').

Koppelingsfase

De smartphones van andere gebruikers waarop de app is geïnstalleerd halen de op de back-end-server beschikbaar gemaakte DKs op. Als de smartphone de DKs heeft opgehaald van de server wordt de verbinding met de server verbroken.

De API genereert (berekent) op de smartphone van de gebruikers voor elk van deze DKs de bijbehorende RPIs/contactcodes en controleert of er een match is met de op de smartphone opgeslagen RPIs/contactcodes, die 14 dagen op de telefoon worden bewaard.

Als er een match is, wordt op basis van ExposureConfiguration-parameters en weegfactoren (zijnde: signaalsterkte, contactduur en eerste ziekte dag) in de app bepaald of er een risicovol contact is geweest. De parameters en weegfactoren worden vastgesteld door VWS, in overleg met RIVM, GGD-en en OMT, en kunnen op basis van nieuwe (wetenschappelijke) inzichten periodiek worden aangepast.

Indien een door VWS, in overleg met RIVM, GGD-en en OMT, vastgestelde drempelwaarde wordt overschreden, geeft de app een signaal dat er sprake is geweest van risicovol contact en ontvangt de gebruiker een notificatie met bijvoorbeeld een advies om scherper te letten op symptomen of om zich bij bepaalde symptomen te laten testen (zie: notificatiefase).

Direct nadat de opgehaalde DKs door de app zijn verwerkt voor het maken van de match en de weging, worden deze verwijderd van de telefoon. In de koppelingsfase controleert de app regelmatig, doorgaans enkele keren per dag, bij de back-end-server of er nieuwe DK's beschikbaar zijn. Is dat het geval dan herhaalt het bovenstaande proces zich.

Notificatiefase

In de notificatiefase genereert de app een notificatie om de gebruiker te informeren over de verhoogde kans op een besmetting met COVID-19 en een advies om zich bij klachten te laten testen op de aanwezigheid van COVID-19. In de notificatie wordt ook de dag van de mogelijke besmetting genoemd. Mocht een gebruiker zich vóór de dag van de mogelijke besmetting dan al hebben laten testen, dan is voor de gebruiker duidelijk dat hij dat, als hij (opnieuw) klachten zou hebben, opnieuw zou moeten doen. Voor de tekst van de notificatie wordt input gevraagd aan de GGD en het RIVM. De tekst van de notificatie kan wijzigen als het overheidsbeleid wijzigt dat ziet op te treffen maatregelen als blijkt dat iemand besmet is.

2. Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

De app wordt zodanig ontwikkeld dat het risico op identificatie van gebruikers via de app zo goed als uitgesloten is. Op de smartphone van de gebruiker zelf worden geen persoonsgegevens verwerkt, ook niet door Apple en Google (zie onderdeel subonderdeel 'Partijen die betrokken zijn, maar niet zelf persoonsgegevens verwerken'). De GGD verwerkt – zoals dat in het 'reguliere proces', buiten de app om, ook het geval is – wel persoonsgegevens bij de vaststelling dat een betrokkene (i.c. een gebruiker van de app) besmet is. Noch voor de GGD noch voor de back-end server noch voor anderen is echter duidelijk welke geüploade TEK's/DK's bij welke (besmet gebleken) gebruiker horen. Dat er – zeer tijdelijk – IP-adressen worden verwerkt maakt dat niet anders. Ter toelichting daarop wordt verwezen naar onderdeel 3, subonderdeel 'Validatiefase' (kort gezegd: het IP-adres wordt in de back-end server gescheiden van de TEKs en tijdelijk op een



ander/afgescheiden gedeelte van de server opgeslagen. Hierdoor is het niet mogelijk te herleiden wie welke informatie heeft verstuurd). Hoewel het risico op identificatie van gebruikers via de app dus zo goed als uitgesloten is, wordt er met het oog op maximale

zorgvuldigheid zekerheidshalve echter van uitgegaan dat er in alle fases van de app wel sprake is van persoonsgegevens.

Afhankelijk van de fase waarin de app zich bevindt hebben de verwerkte gegevens een wisselend karakter. Om die reden zijn de verschillende fases los beschreven.

Installatiefase

Geen persoonsgegevens⁷

Uitwisselingsfase

Gewone persoonsgegevens:

- TEKs
- RPIs/contactcodes
- signaalsterkte en de contactduur

In deze fase worden uitsluitend (1) RPIs/contactcodes uitgewisseld tussen gebruikers van de app die in elkaars nabijheid zijn geweest met de daarbij behorende signaalsterkte zowel uitgezonden als ontvangen, en de duur van het bluetoothcontact, en (2) de eigen TEKs opgeslagen op de eigen smartphone. Deze uitwisseling gebeurt zonder tussenkomst van een server.

Validatiefase

Bijzondere Persoonsgegevens

- TEKs en DKs
- autorisatiecode
- signaalsterkte en de contactduur
- eerste ziektedag
- TransmissionRiskValue (high, mid, low)
- IP-adres

Koppelingsfase

Bijzondere persoonsgegevens

- TEKs en DKs
- RPIs/contactcodes
- signaalsterkte en de contactduur
- TransmissionRiskValue (high, mid, low)

Notificatiefase

Bijzondere persoonsgegevens:

- de notificatie aan de gebruiker dat hij mogelijk besmet is met COVID-19
- de dag dat de gebruiker in contact is geweest met een besmet persoon (wordt vermeld in de notificatie)

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.



Installatiefase

In de installatiefase vindt geen verwerking van persoonsgegevens plaats door VWS of de GGD-en.⁸

Uitwisselingsfase

In de uitwisselingsfase worden de eigen TEKs van de gebruiker bewaard, alsmede ontvangen RPIs/contactcodes, met de daarbij behorende signaalsterkte zowel uitgezonden als ontvangen, en de duur van het bluetoothcontact.

Om het risico op identificatie van gebruikers zoveel mogelijk uit te sluiten wordt bij de uitwisseling van TEKs het MAC-adres van de smartphone vervangen door een random gegenereerde code, een pseudo MAC-adres, die evenals de TEKs elke 10 – 20 minuten verandert.

Validatiefase

In de validatiefase worden geüploade TEKs van gebruikers die positief zijn getest op COVID-19 geconverteerd naar DKs en vervolgens gevalideerd aan de hand van de autorisatiecode die de GGD in de GGD-portaal van de app heeft vastgelegd. Voor elke DK wordt de datum van de eerste ziektedag vergeleken met de datum van de TEKs. Op basis daarvan wordt door de server een zgn. TransmissionRiskValue (high, mid, low) bepaald.

Tijdens de validatiefase worden voor beheers- en beveiligingsdoeleinden IP-adressen verwerkt. Een dergelijke verwerking is inherent aan het gebruik van internet en IP-technologie. Zodra de data via internet aankomt bij de Belastingdienst (die back-end server draait, zie hierna onderdeel 5) worden de TEKs/DKs doorgestuurd naar de server zonder dat daar een link met het IP-adres te maken is. De verkeersgegevens, waaronder IP-adressen, worden zonder de TEKs/DKs geanalyseerd op mogelijk aanvallen. Als gevolg van de scheiding van verkeersgegevens en TEKs/DKs kunnen de onderscheiden

⁷ Om de app te downloaden moeten gebruikers toegang hebben tot de Apple App Store of de Google Play Store. Om deze toegang te verkrijgen wordt van gebruikers gevraagd (persoons)gegevens, zoals een emailadres, te verstrekken aan Apple resp. Google. Deze gegevens worden in het kader van de notificatie app niet gebruikt. Als zodanig valt de verwerking daarvan buiten het bereik van deze DPIA.

⁸ Zie vorige voetnoot.

gegevens niet aan elkaar worden gerelateerd, evenmin is op de server te achterhalen van welke gebruiker de TEKs/DKs afkomstig zijn.

Daartoe zijn een viertal vertrouwelijke maatregelen genomen (TLP: AMBER).

Koppelingsfase

In de koppelingsfase worden DKs van gebruikers die positief zijn getest op COVID-19 beschikbaar gemaakt voor download vanaf de back-end server. Vervolgens worden die DKs gedownload door de apps die in gebruik zijn, met het doel na te kunnen gaan of zij corresponderende RPIs/contactcodes hebben ontvangen in de afgelopen veertien dagen. Als er een match is, wordt op basis van de door VWS, in overleg met RIVM, GGD-en en OMT, vastgestelde parameters en weegfactoren in de app afgewogen of er een risicovol contact is geweest, dat aanleiding kan zijn voor het doen van een notificatie aan de desbetreffende gebruikers.

Notificatiefase

In de notificatie wordt aan de gebruiker gemeld dat hij mogelijk besmet is met COVID-19, inclusief vermelding van de dag dat die gebruiker in contact is geweest met een besmet persoon.

4. Verwerkingsdoeleinden



Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Doel van de voorgenomen gegevensverwerkingen is om de bron- contactopsporing van de GGD-en te ondersteunen met een app die gebruikers waarschuwt als zij risicovol contact hebben gehad met een op COVID-19 positief getest persoon. Hierdoor neemt de kans toe dat potentieel geïnfecteerde personen eerder in beeld komen en – daarmee – dat een exponentiële uitbraak van het virus sneller wordt afgeremd.

Alle gegevens die worden verwerkt zijn strikt noodzakelijk om het bovenstaande doel op betrouwbare en veilige wijze te verwezenlijken.

5. Betrokken partijen



Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen.

Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Verwerkingsverantwoordelijken:

In een wetsvoorstel dat de inzet van de app expliciteert wordt, onder andere naar aanleiding van het advies van de AP en om mogelijke onduidelijkheid daarover uit te sluiten, expliciet opgenomen wie de verwerkingsverantwoordelijke is voor de notificatieapp.

De verwerkingsverantwoordelijkheid is op twee niveaus neergelegd. De Minister van VWS is de verwerkingsverantwoordelijke voor gegevensverwerkingen in het kader van de inrichting en het beheer van de notificatieapp en de AVG-verplichtingen die daarbij horen. Er wordt hiermee aangesloten bij zijn taken op grond van de artikelen 3 en 7 Wpg, zijnde: het geven van leiding aan infectieziektebestrijding, de bevordering van de kwaliteit en doelmatigheid van de publieke gezondheidszorg en de instandhouding en verbetering van de landelijke ondersteuningsstructuur.

De GGD is gelet op artikel 6, eerste lid, onderdeel c, jo. artikel 14 Wpg belast met bron- en contactopsporing. De GGD wordt als verwerkingsverantwoordelijke aangemerkt voor wat betreft het uitvoering geven aan de informatieverstrekking aan en het voldoen aan de zgn. AVG-rechten van de gebruikers van wie door middel van de notificatieapp persoonsgegevens worden verwerkt. Het gaat dan onder meer om de plicht om gebruikers te informeren, het recht op inzage en het recht op rectificatie. Dit omdat het onwenselijk wordt geacht dat de minister ook in deze gevallen als verwerkingsverantwoordelijke te beschouwen, aangezien hij dan juist persoonsgegevens ten behoeve van de notificatieapp zou gaan verwerken terwijl dat niet nodig en daarmee vanuit privacyrechtelijk perspectief niet wenselijk is.

Verwerkers:

De Belastingdienst:

De Belastingdienst verzorgt de technische exploitatie van de back-end server. VWS maakt (ook namens de GGD'en) verwerkersafspraken met de Belastingdienst. Voor het publiceren c.q. het voor downloaden beschikbaar maken van de DKs maakt de Belastingdienst gebruik van het Microsoft Azure platform van Microsoft. Deze bevinden zich binnen de Europese Economische Ruimte (zowel de primaire als de fail-over systemen).

De Belastingdienst is (sub)verwerkersovereenkomsten en service level agreements aangegaan met Microsoft.

Partijen die betrokken zijn, maar niet zelf persoonsgegevens verwerken:

Apple en Google:

Om gebruik te kunnen maken van de notificatie app moeten gebruikers, afhankelijk van het type smartphone waarvan gebruik wordt gemaakt, deze downloaden uit de Apple App Store (iOS) of Google Play Store (Android). De beide downloadomgevingen zijn zoals bekend naar hun aard publiek beschikbaar.

Om de ontwikkeling van de app mogelijk te maken hebben Apple en Google een API ontwikkeld.⁹ Deze API maakt mogelijk dat de app op basis van het DP3T protocol¹⁰ kan functioneren op hun besturingssystemen (iOS resp. Android). De API en het systeem waarvan de API onderdeel uitmaakt zijn zo ontworpen en opgezet dat Apple en Google geen toegang kunnen hebben tot de gegevens die betrekking hebben op de gebruikers (d.w.z. de gegevens in de app van VWS, waar Apple en Google geen toegang toe hebben). Dit blijkt uit de documentatie die Apple en Google daarover hebben bekendgemaakt. Aldus het document Exposure Notification. Frequently Asked Questions, v1.1, May 2020:¹¹

The system was also designed so that Apple and Google do not have access to information related to any specific individual.

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.

De implementatiesoftware van het DP3T protocol (de app van VWS) verwerkt de TEKs, DKs en RPIs/contactcodes, én kan een risicoscore bepalen aan de hand van een in de app opgenomen set parameters en weegfactoren. De parameters en weegfactoren worden vastgesteld door VWS, in overleg met RIVM, GGD-en en OMT, en kunnen op basis van nieuwe (wetenschappelijke) inzichten periodiek worden aangepast.

Er is sprake van de verwerking van (pseudonieme) persoonsgegevens (RPIs/contactcodes) van betrokkene op de smartphones van andere gebruikers, en de verwerking van gedownloade DKs en op basis daarvan gegenereerde (berekende) contactcodes. Deze gegevens, die zich in de app van VWS bevinden, zijn niet toegankelijk voor Apple en Google.

Ontvanger:

De app op de smartphone van de gebruiker haalt DKs op van de back-end-server, en genereert (berekent) daarmee de RPIs/contactcodes die kunnen worden vergeleken met de RPIs/contactcodes die zijn opgeslagen op de desbetreffende smartphone (koppelingsfase). Het is voor de gebruiker niet mogelijk om de TEKs, DKs en RPIs/contactcodes en daarbij behorende parameters in te zien.

6. Belangen bij de gegevensverwerking i

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenoemde gegevensverwerkingen.

Het belang van VWS en de GGD-en bij de inzet van de app, is de ondersteuning die de app biedt bij het uitvoeren van de bron- en contactopsporing gedurende de COVID-19 crisis. Gelet op de nationale volksgezondheid is het van belang dat de verspreiding van het COVID-19 virus snel en adequaat wordt gesignaleerd, en dat mensen worden geïnformeerd over een mogelijke besmetting, zodat deze passende maatregelen kunnen treffen om verdere verspreiding te voorkomen.

Het belang van de betrokkenen bij de app is dat zij op eenvoudige wijze en met een hoge mate van anonimiteit geïnformeerd worden over een verhoogde besmettingskans en zich daardoor eerder laten testen op de aanwezigheid van Covid-19.

Apple en Google zouden ook belang bij de gegevensverwerkingen kunnen hebben, al verwerken zij als gezegd zelf geen persoonsgegevens. Dat Apple en Google de API hebben ontwikkeld zou in positieve zin kunnen bijdragen aan de wijze waarop zij in het maatschappelijk verkeer worden gezien.

7. Verwerkingslocaties i

Benoem in welke landen de voorgenoemde gegevensverwerkingen plaatsvinden.

Voor zover gegevens worden verwerkt op de smartphone van de gebruiker is de verwerkingslocatie afhankelijk van de fysieke locatie van de betreffende smartphone.

Gelet op de Europese interoperabiliteitsambities voor de verschillende nationale tracing apps, is het waarschijnlijk dat de lokale gegevensverwerking op de smartphone binnen de gehele Europese Economische Ruimte (EER) kan plaatsvinden.

Voor zover gegevens worden verwerkt op de back-end-server vindt dat plaats in Nederland. Afhankelijk van de gekozen infrastructuur op Europees niveau bestaat de mogelijkheid dat persoonsgegevens ook worden opgeslagen buiten Nederland. In dat geval zal deze parallelle opslaglocatie zich in elk geval binnen de EER bevinden.

⁹ De documentatie over de door Apple en Google ontwikkelde API's is te vinden via www.apple.com/covid19/contacttracing (laatst. geraadpl. 1 juli 2020); Exposure Notification. FAQ, v1.1 May 2020; Exposure Notification. Cryptography Specification, v1.2 April 2020; Exposure Notification. Bluetooth Specification, v1.2, April 2020.

¹⁰ DP3T wordt omschreven als "a secure, decentralized, privacy-preserving proximity tracing system. Its goal is to simplify and accelerate the process of identifying people who have been in contact with an infected person, thus providing a technological foundation to help slow the spread of the SARS-CoV-2 virus. The system aims to minimise privacy and security risks for individuals and communities and guarantee the highest level of data protection." De documentatie over DP3T is te vinden in het DP3T Repository op <https://github.com/DP-3T/documents> (laatst. geraadpl. 1 juli 2020).

¹¹ Exposure Notification. Frequently Asked Questions, v1.1, May 2020, par. 6 en 7, te vinden via www.apple.com/covid19/contacttracing (laatst. geraadpl. 1 juli 2020)

Voor het publiceren c.q. het voor downloaden beschikbaar maken van de DKs maakt de Belastingdienst gebruik van het Microsoft Azure platform van Microsoft. Deze bevinden zich binnen de Europese Economische Ruimte (zowel de primaire als de fail-over systemen).

8. Techniek en methode van gegevensverwerking



Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi)geautomatiseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Installatiefase

Voor de installatie van de app wordt gebruik gemaakt van de app store van Apple (in het geval van een smartphone met iOS als besturingssysteem) of Google (in het geval van een smartphone met Android als besturingssysteem).

Uitwisselingsfase

In de uitwisselingsfase is het belangrijkste technische middel de door Google en Apple in hun besturingssystemen geïmplementeerde variant van het D-3T protocol. DP3T staat voor "Decentralised, Privacy-Preserving Proximity Tracing". Zoals de naam al aangeeft gaat het om nabijheidsdetectie zonder dat specifieke locaties worden opgeslagen. Om de voorgenomen Europese interoperabiliteit van de verschillende nationale apps te kunnen waarborgen, zal te zijner tijd daarom mogelijk een landcode moeten worden toegevoegd vanuit de app.

De nabijheidsdetectie maakt gebruik van een variant van het Bluetooth protocol, Bluetooth Low Energy (BLE). De nabijheidsdetectie is erop gebaseerd dat het ontvangen BLE-signaal van een andere smartphone vergeleken wordt met de door diezelfde smartphone uitgezonden berichten die naast de RPIs/contactcodes ook de uitgezonden signaalsterkte bevatten. Het verschil tussen de sterkte van het uitgezonden en het ontvangen BLE-signaal wordt gebruikt als indicator voor de fysieke nabijheid. Gecombineerd met de duur van het contact kan hiermee achteraf een inschatting gegeven worden van het eventuele besmettingsrisico van COVID-19.

Validatiefase

Voor de validatie wordt gebruik gemaakt van door VWS ontwikkelde software op infrastructuur van de Belastingdienst.

Het voor downloaden beschikbaar maken van de DKs vindt plaats met standaard webtechnologie (nl. content delivery network en storage), waarbij voor de flexibiliteit en de schaalbaarheid gebruik wordt gemaakt van het Microsoft Azure platform zoals gecontracteerd door de Belastingdienst.

Koppelingsfase

Voor de koppeling wordt gebruik gemaakt van het DP3T protocol, dit vindt plaats op de smartphone zelf.

Notificatiefase

Notificaties worden aan de hand van het besturingssysteem van de betreffende smartphone (iOS of Android), op de smartphone gegenereerd en via een zgn. pushmelding aan de gebruiker doorgegeven.

Geautomatiseerde besluitvorming

Van geautomatiseerde besluitvorming, in de zin van artikel 22, eerste lid, AVG, is in de notificatie app geen sprake. Dit omdat er vanaf het moment van installatie tot het moment van notificatie op verschillende momenten sprake is van menselijke tussenkomst:

1. Er wordt middels menselijke tussenkomst (namelijk via tussenkomst van de GGD) vastgesteld of sprake is van een besmetting.
2. Als sprake is van een besmetting wisselt de betreffende gebruiker een in de app gegenereerde validatiecode uit met de GGD, die zowel de gebruiker als de GGD naar de back-end server moeten sturen, voordat de back-end de door de gebruiker toegezonden TEKs accepteert en deze – nadat ze naar DKs zijn omgezet – voor download ter beschikking stelt. De GGD stuurt naast de validatiecode ook de door de gebruiker aan de GGD doorgegeven eerste dag waarop de gebruiker ziekteverschijnselen kreeg naar de back-end server, mits de gebruiker daar toestemming voor geeft. Ook hier is dus sprake van menselijke tussenkomst.

Zou echter al aangenomen moeten worden dat wel sprake is van geautomatiseerde besluitvorming die bovendien aanmerkelijke gevolgen heeft voor de betrokkene (in dit geval voor de gebruiker die een notificatie krijgt dat hij mogelijk besmet is met COVID-19), dan geldt dat die geautomatiseerde besluitvorming noodzakelijk is voor de vervulling van een taak van algemeen belang, te weten de beheertaak van de minister als bedoeld in artikel 3 van de Wpg en de bron- en contactopsporingstaak van de GGD als bedoeld in artikel 6, eerste lid, onderdeel c, jo. artikel 14 Wpg. Dat betekent dat het verbod van artikel 22, eerste lid, AVG niet geldt (zie art. 22, tweede lid, aanhef en onderdeel b AVG jo. art. 40, eerste lid, UAVG jo. art. 3, art. 6 en art. 14 Wpg).

In aanvulling daarop kan er, ten overvloede, nog op worden gewezen dat het verbod van artikel 22, eerste lid, AVG hoe dan ook niet van toepassing is omdat de gebruiker bij de installatie van de app ermee heeft ingestemd dat hij een notificatie kan ontvangen dat hij (mogelijk) besmet is.

9. Juridisch en beleidsmatig kader



Benoem de wet en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

Het relevante juridische kader is neergelegd in de Wet publieke gezondheid (Wpg). De belangrijkste artikelen hieruit zijn de artikelen 3, 6 en 7 Wpg

De inzet van de notificatieapp maakt zo onderdeel uit van de bron- en contactopsporing van de GGD zoals geregeld in artikel 6, eerste lid, onderdeel c, jo. artikel 14 Wpg. Met de app wordt de GGD ondersteund in de uitvoering van die taak.

De GGD heeft op grond van artikel 6, eerste lid, onderdeel c jo. artikel 14 Wpg de taak om bron- en contactopsporing te doen bij meldingen van besmetting met een infectieuze ziekte zoals het Covid-19. De uitvoering hiervan is vormvrij en de GGD geeft hier de afgelopen jaren in de praktijk dan ook op verschillende manieren invulling aan, zowel analoog als digitaal.

Op basis van artikel 3, eerste lid, Wpg heeft de minister de taak om de kwaliteit en doelmatigheid van de publieke gezondheidszorg te bevorderen en zorg te dragen voor de instandhouding en verbetering van de landelijke ondersteuningsstructuur.

Het OMT heeft geadviseerd om met het oog op het intensievere testbeleid de mogelijkheden voor ondersteuning van bron- en contactopsporing met behulp van mobiele applicaties te onderzoeken.¹² Ook de Tweede Kamer heeft in de breed aangenomen motie Jetten c.s.¹³ overwogen dat het gebruik van apps kan bijdragen aan het beheersen van het virus. De inzet van dergelijke apps heeft ook de aandacht van andere Europese lidstaten en de Europese Commissie.¹⁴

Met het invoeren van de app als ondersteunend middel voor bron- en contactopsporing wordt uitvoering gegeven aan de taak van de GGD-en en de minister, aan het advies van het OMT en aan de aangenomen motie van de Tweede Kamer.

10. Bewaartermijnen



Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

¹² Bijlage 929506 bij *Kamerstukken II 2019/20, 25 295*, nr. 219.

¹³ *Kamerstukken II 2019/20, 25 295*, nr. 223.

¹⁴ https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

Installatiefase

n.v.t.

Uitwisselingsfase

De persoonsgegevens uit de uitwisselingsfase worden veertien dagen bewaard. De gebruiker kan desgewenst de bewaartermijn verkorten, want heeft de mogelijkheid om alle gegevens te verwijderen of de hele app te verwijderen waardoor ook alle opgeslagen gegevens op de telefoon worden verwijderd.

Voor de bewaartermijnen van veertien dagen is gekozen omdat contacten met COVID-19 besmette personen die langer dan veertien dagen in het verleden liggen niet meer relevant zijn voor het beoordelen van de vraag of er een verhoogd besmettingsrisico is, aangezien een gebruiker na 14 dagen al ziekteverschijnselen moet hebben.

Validatiefase

In de validatiefase kan de gebruiker, als de GGD heeft vastgesteld dat hij of zij is geïnfecteerd, ervoor kiezen om de eigen TEKs, tezamen met een unieke, door de app gegenereerde autorisatiecode naar de back-end-server te sturen. Deze autorisatiecode moet door de GGD worden gevalideerd en daartoe plaatst de GGD deze code in het GGD-portaal van de app.

In de situatie dat om een of andere reden, bijvoorbeeld verbindingsproblemen, de autorisatiecode niet door de GGD is geplaatst in de GGD-portaal, wordt de door de gebruiker naar de back-end-server gestuurde code gedurende 24 uur op deze server bewaard.

Eenzelfde bewaartermijn wordt gehanteerd in de situatie dat de GGD de autorisatiecode in de GGD-portaal heeft geplaatst maar er geen corresponderende code door de gebruiker naar de back-end-server is gestuurd.

De geuploade TEKs en DKs en de eerste ziektedag worden 24 uur op back-end server bewaard. Voor deze bewaartermijn van 24 uur is gekozen omdat het DP3T protocol een nachtelijke nazending van TEKs van de laatste dag van de upload vereisen. Pas daarna kunnen dus alle relevante DKs voor download ter beschikking worden gesteld.

Als gezegd worden in de validatiefase ook IP-adressen verwerkt, op een wijze waardoor het niet mogelijk is te herleiden wie welke informatie heeft verstuurd (zie onderdeel 3, subonderdeel 'Validatiefase'). Het IP-adres wordt na zeven dagen vernietigd. Het IP-adres wordt tijdelijk verwerkt ten behoeve van de beveiligingsfunctionaliteit van de application firewall, het detecteren van aanvallen, etc.

Koppelingsfase

De persoonsgegevens die verwerkt worden in de koppelingsfase worden direct nadat de opgehaalde DKs verwerkt zijn voor het maken van de match en de weging, verwijderd van de smartphone.

Notificatiefase

De notificatie blijft staan, totdat de gebruiker deze wegklikt. Na wegklikken blijven er van de notificatie geen sporen achter.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de DPIA is in het bijzonder juridische expertise nodig.

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

Zowel de minister als de GGD-en maken gebruik van de verwerkingsgrondslag van artikel 6, eerste lid, onderdeel e, AVG, zijnde de verwerking die noodzakelijk is voor de uitoefening van een taak van algemeen belang.

Voor de minister gaat het om de taken hem opgedragen in artikel 3 Wpg, nl. de bevordering van de kwaliteit en doelmatigheid van de publieke gezondheidszorg en het zorgdragen oor de instandhouding en verbetering van de landelijke ondersteuningsstructuur.



De GGD heeft op grond van artikel 6, eerste lid, onderdeel c, jo. artikel 14 Wpg de taak om bron- en contactopsporing te verrichten bij meldingen van besmetting met een infectieuze ziekte zoals Covid-19.

In andere lidstaten, zoals Duitsland, is ervoor gekozen om voor de verwerkingsgrondslag uit te gaan van de toestemming van de gebruiker, als bedoeld in artikel 6, eerste lid, onderdeel a, AVG. Voor de notificatie app is daarvoor niet gekozen omdat er, zeker in de relatie van burger en overheid, al snel de vraag kan opkomen of de toestemming in vrijheid is gegeven.¹⁵ De verwerkingsgrondslag van het algemeen belang, als bedoeld in artikel 6, eerste lid, onderdeel e, AVG is daarom passender. Dit doet er niet aan af dat de gebruiker op verschillende momenten gevraagd wordt in te stemmen met de verwerkingen die plaats kunnen vinden bij het gebruik van de app, zoals bij het downloaden en installeren van de app op de eigen smartphone, bij het mogelijk maken dat de app bepaalde gebruiksrechten krijgt en als de gebruiker de mogelijkheid krijgt om de TEKs met autorisatiecode naar de back-end-server te sturen. Op deze wijze wordt geborgd dat het gebruik van de app vrijwillig is. Als gezegd heeft de gebruiker ook op ieder moment de mogelijkheid om alle gegevens te verwijderen of de hele app te verwijderen waardoor ook alle opgeslagen gegevens op de telefoon worden verwijderd.

Er wordt gewerkt aan een wetsvoorstel waarin het direct of indirect verplicht gebruik van de app expliciet wordt verboden.

Terzijde: Uit artikel 11.7a van de Telecommunicatiewet volgt dat het via een elektronisch communicatienetwerk (zoals internet) of draadloos transmissiesysteem (zoals bluetooth) plaatsen of lezen van informatie op een randapparaat zoals een smartphone, ongeacht of er sprake is van persoonsgegevens, uitsluitend is toegestaan op voorwaarde dat de gebruiker daarvoor toestemming heeft verleend én is voorzien van duidelijke en volledige informatie. Deze bepaling bevat met andere woorden voor wat betreft de notificatieapp een informatieplicht en een toestemmingsvereiste voor het opslaan van de notificatieapp op een smartphone, voor het uitwisselen van de contactcodes tussen deze smartphone en andere smartphones in de nabijheid die ook gebruik maken van de app, en voor het uitsturen van een eventuele melding van de besmetting naar de server.

De notificatieapp wordt zodanig ingericht dat aan deze vereisten is voldaan. Zo is het gebruik van de notificatieapp vrijwillig. Daarbij is van belang dat het niet geven van toestemming niet leidt tot ondermijning van de keuzevrijheid; mensen die de notificatieapp niet willen gebruiken kunnen zich bij klachten gewoon laten testen en (vrijwillig) meewerken aan analoge bron- en contactopsporing. Verder wordt er bij het downloaden van de notificatieapp specifiek toestemming gevraagd voor zowel het gebruik van de app als de api. Daarbij zal duidelijk worden gemaakt dat de toestemming ziet op (1) het opslaan van de notificatieapp, (2) het opslaan van de eigen TEK's, (3) het verzenden van de eigen contactcodes aan gebruikers in de nabijheid en (4) het opslaan van contactcodes van andere gebruikers. Vervolgens wordt nadat een besmetting is geconstateerd toestemming gevraagd voor (5) het versturen van de TEK's, contactcodes en dag van ziekteverschijnselen naar de server.

¹⁵ Zie ook overw. 43 uit de Preambule bij de AVG.

12. Bijzondere persoonsgegevens i

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

De RPIs/contactcodes en TEKs kunnen in de validatiefase en koppelingsfase beschouwd worden als (zij het vergaand gepseudonimiseerde) gezondheidsgegevens.

Onder omstandigheden bestaat dus de mogelijkheid dat TEKs en DKs gekwalificeerd kunnen worden als gegevens betreffende de gezondheid¹⁶, waarvoor een verwerkingsverbod geldt op grond van artikel 9, eerste lid, AVG. In dat geval moet het verwerkingsverbod worden 'doorbroken' op grond van één van de gronden geformuleerd in artikel 9, tweede lid, AVG.

Voor de notificatie app kan gebruik worden gemaakt van de doorbrekingsgrond van artikel 9, tweede lid, onderdeel i, AVG. Deze bepaling, in combinatie met de Wpg, biedt een uitzondering op het verwerkingsverbod voor bijzondere persoonsgegevens om redenen van algemeen belang op het gebied van de volksgezondheid.¹⁷ Uit overweging 46 AVG blijkt dat daaronder moeten worden verstaan de verwerking van bijzondere persoonsgegevens die de vitale belangen van betrokkenen dienen, bijvoorbeeld verwerking die noodzakelijk is voor het monitoren van een epidemie en de verspreiding daarvan.¹⁸

13. Doelbinding i

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

Er is geen sprake van verdere verwerking door VWS of de GGD-en.

14. Noodzaak en evenredigheid i

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?

¹⁶ Artikel 4, aanhef en onder 15, AVG.

¹⁷ De definitie van de term 'volksgezondheid' die in dit kader wordt gehanteerd vloeit voort uit Verordening (EG) 1338/2008, en omvat het volgende: Artikel 3, aanhef en onder c, Verordening (EG) 1338/2008 c) "volksgezondheid": alle elementen in verband met de gezondheid, namelijk gezondheidstoestand, inclusief morbiditeit en beperkingen, de determinanten die een effect hebben op die gezondheidstoestand, de behoeften aan gezondheidszorg, middelen ten behoeve van de gezondheidszorg, de verstrekking van en de universele toegang tot gezondheidszorg, alsmede de uitgaven voor en de financiering van de gezondheidszorg, en de doodsoorzaken;

¹⁸ Overweging 46 AVG.

b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?

Proportionaliteit

In de huidige fase van de bestrijding van COVID-19, waarin het aantal nieuwe besmettingen, ziekenhuisopnames en nieuwe opnames op de IC-afdelingen is afgenomen, is Nederland in een overgangsfase terechtgekomen waarin beperkende maatregelen worden versoepeld en het aantal contacten tussen personen geleidelijk weer toeneemt. Deze versoepelingen vergen een slimme controle-strategie bestaande uit een combinatie van begeleidende maatregelen en de medewerking van de gehele bevolking.

Omdat het afbouwen van de beperkende maatregelen alleen mogelijk is als verdere infecties zoveel mogelijk worden voorkomen is er een cruciale rol weggelegd voor de bron- en contactopsporing door de GGD, zo nodig op grote schaal. Daarbij is gezocht naar mogelijkheden om grootschalige bron- en contactopsporing te ondersteunen, bijvoorbeeld op digitale wijze aangezien de GGD'en al langere tijd gewend zijn digitaal te werken (zie de 'GGD-appstore'). Net als in de ons omringende landen is hierbij de keuze gevallen op een notificatieapp.

Het OMT heeft ook geadviseerd om met het oog op het intensievere testbeleid de mogelijkheden voor ondersteuning van bron- en contactopsporing met behulp van mobiele applicaties te onderzoeken.¹⁹ Ook de Tweede Kamer heeft in de breed aangenomen motie Jetten c.s. overwogen dat het gebruik van apps kan bijdragen aan het beheersen van het virus.²⁰ De inzet van dergelijke apps heeft ook de aandacht van andere Europese lidstaten en de Europese Commissie.²¹

De GGD heeft de wettelijke taak tot het doen van bron- en contactopsporing. Bron- en contactopsporing is vormvrij en moet breed worden opgevat. De GGD moet immers kunnen differentiëren naar wat afhankelijk van de omstandigheden van het geval de beste aanpak is.

Voor de bestrijding van de epidemie geldt dat het doel van bron- en contactopsporing het beste kan worden bereikt als zoveel mogelijk mensen die risicovol in de nabijheid van een geïnfecteerde persoon zijn geweest zo snel mogelijk kunnen worden gewaarschuwd. Dit is alleen mogelijk als mensen voorafgaand aan een besmetting reeds (zo privacyvriendelijk mogelijk) bijhouden in wiens nabijheid zij zijn geweest. Het door middel van de app uitwisselen en opslaan van contactcodes en TEKs/DKs is derhalve onlosmakelijk verbonden met de bron- en contactopsporing door de GGD.

Deze wettelijke taak van de GGD dient een algemeen belang op het gebied van volksgezondheid. De door de GGD verrichtte bron- en contactopsporing is essentieel

¹⁹ Bijlage 929506 bij Kamerstukken II 2019/20, 25 295, nr. 219.

²⁰ Kamerstukken II 2019/20, 25 295, nr. 226.

²¹ https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

voor het doorbreken van de keten van infecties en het voorkomen van verdere infecties en levert daarmee een cruciale bijdrage aan de bestrijding van het virus.

Dit sluit aan bij het uitgangspunt van de EDPB dat 'het rechtskader voor gegevensbescherming is ontworpen met flexibiliteit voor ogen en als zodanig een efficiënte respons mogelijk maakt die de pandemie indamt en de fundamentele mensenrechten en vrijheden beschermt'.

Verder wordt opgemerkt dat bij constatering van een (mogelijke) infectie door de GGD sprake is van een behandelrelatie tussen een geïnfecteerde burger en de GGD. Artikel 7:457 BW voorziet in een geheimhoudingsplicht daarvoor. Strikt genomen ziet dit niet op de app als zodanig, maar op het werk van de GGD, maar dat werk speelt in zekere zin wel een rol, omdat een gebruiker pas met de vaststelling door de GGD van een besmetting succesvol TEKs naar de back-end server kan uploaden.

De AVG bepaalt dat alle verwerkingen van persoonsgegevens moeten voldoen aan de vereisten van proportionaliteit en subsidiariteit. Dit houdt kort gezegd in dat ten eerste het doel en de aard en omvang van de gegevens die voor dat doel worden verwerkt met elkaar in verhouding moeten zijn en ten tweede dat altijd moet worden gekozen voor de minst ingrijpende verwerking van persoonsgegevens.

Zoals eerder toegelicht wordt de app ingezet om bron- en contactopsporing door de GGD te ondersteunen en zo het virus sneller en beter te kunnen bestrijden:

(1) Personen die in de nabijheid van geïnfecteerde personen zijn geweest worden sneller bereikt

Het spreekt voor zich dat de analoge methode van contactopsporing niet alleen een arbeidsintensieve bezigheid is, maar ook beperkingen met zich brengt voor wat betreft de doeltreffendheid en de te verwerken aantallen meldingen. In veel gevallen moet worden onderkend dat mensen zich niet altijd exact herinneren met wie zij allemaal contact hebben gehad over een bepaalde tijdsperiode, laat staan dat men van al die personen de contactgegevens zou hebben. Ook vergt het van de GGD veel tijd en mankracht om de contactpersonen te bereiken, waardoor geïnfecteerde personen intussen opnieuw andere personen kunnen besmetten.

(2) Het bereik van het contactonderzoek wordt in belangrijke mate vergroot

Iemand kan in de nabijheid zijn geweest van mensen die hij überhaupt niet kent en waarvan dus ook geen contactgegevens bekend zijn. Denk hierbij bijvoorbeeld aan een bezoek aan een speeltuin of park, een reis met het openbaar vervoer of deelname aan een demonstratie waarbij men andere mensen tegenkomt waarvan de identiteit onbekend is en ook niet via fysiek onderzoek te achterhalen is. Daarnaast is contact met een geïnfecteerd persoon om contacten te achterhalen niet altijd mogelijk bijvoorbeeld omdat die persoon fysiek daartoe niet in staat is.

De ernst en de gevolgen van het virus, zowel voor individuen persoonlijk als op landelijke schaal leiden tot de conclusie dat het gedurende een beperkte termijn van 14

dagen verwerken van een zeer beperkt aantal gegevens die bovendien zo veel mogelijk lokaal op de smartphones van gebruikers worden opgeslagen proportioneel is.

Mensen kunnen ernstig ziek worden of zelfs overlijden, mensen kunnen niet meer het leven leiden zoals zij gewend waren en ondervinden daarvan ook psychisch de gevolgen van. Daarnaast loopt de economie grote schade op. De tijd is daarbij een belangrijke factor: hoe sneller en diepgaander het virus opgespoord kan worden, des te beter en effectiever het virus bestreden kan worden.

De inzet van moderne digitale middelen zoals de app is daarom noodzakelijk en proportioneel.

Subsidiariteit

De inzet van de app zal naar verwachting een grote bijdrage kunnen leveren aan de bestrijding van de epidemie en is daarom als één van de in te zetten middelen van cruciale betekenis (zie ook hierna over effectiviteit en evaluatie). Een minder ingrijpend alternatief zou erin kunnen zijn gelegen dat wordt volstaan met enkel de analoge bron- en contactopsporing, die weliswaar nodig blijft naast de inzet van de app, maar waarmee niet eenzelfde ruime groep mensen kan worden bereikt en vervolgens snelle en gerichte actie kan worden ondernomen. Zeker voor wat betreft het waarschuwen van mensen die men niet kent is geen goed alternatief voorhanden.

De verwerking van (persoons)gegevens is beperkt tot het strikt noodzakelijke. Voor zover als sprake is van verwerking van persoonsgegevens, gaat het om sterk gepseudonimiseerde persoonsgegevens. Daarnaast zijn ook verschillende andere passende technische en organisatorische beveiligingsmaatregelen getroffen (zie daarover ook onderdeel 16 en 17).

Effectiviteit en evaluatie

De doeltreffendheid van de notificatieapp is exponentieel evenredig met het aantal personen dat eenzelfde app installeert en activeert. Fundamenteel vereiste voor een doeltreffende exit-strategie waarbij een notificatieapp wordt ingezet, is dan ook het vertrouwen van de burger in een dergelijke app en de grootst mogelijke vrijwillige deelname van de burger hieraan. Het gebruik ervan moet dan ook met de strengste waarborgen omkaderd zijn.

Simulatiemodellen en eerste wetenschappelijke inzichten suggereren dat, zelfs bij inachtneming van beperkt gebruik, de introductie van een notificatieapp kan bijdragen aan de reductie van het aantal verdere besmettingen en het reduceren van de tijd tussen besmetting en signalering van andere geïnfecteerden.²² Daarnaast wordt de notificatieapp voordat deze landelijk in gebruik wordt genomen getest op effectiviteit, zowel technisch (stelt de app inderdaad risicovolle nabijheid vast?) als op gebruikersvriendelijkheid en toegankelijkheid. Daarbij wordt ook een vergelijking gemaakt met de testresultaten uit andere landen, zoals Duitsland en Zwitserland. Het

²² <https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown> . Zie ook <https://pubmed.ncbi.nlm.nih.gov/32234805>.

gaat eerst om testen in een laboratorium gevolgd door praktijktesten, eerst op kleine schaal en vervolgens in de regio Twente. Daarbij zullen ook medewerkers van de GGD en specifieke doelgroepen zoals slechthorenden/doven, slechtzienenden/blinden en anderstaligen worden betrokken. Zoals ook de EDPB aanbeveelt, zal gedurende het gebruik van de notificatieapp onderzoek gedaan worden naar de effectiviteit en worden buitenlandse ontwikkelingen op dit vlak nauwgezet gevolgd. De werking van de notificatie app zal verder worden gemonitord aan de hand van een vooraf vastgesteld evaluatieprotocol. Daarbij wordt periodiek bekeken of er daadwerkelijk sprake is van breder, sneller en efficiënter opsporen van besmette mensen en of er wellicht niet beoogde neveneffecten zijn die om bijsturing vragen. Deze monitoring leidt zo nodig tot aanpassingen en bijstellingen van de notificatieapp, bijvoorbeeld door het aanpassen van de eerder genoemde waardes die zijn toegekend aan de parameters waarmee wordt berekend of er sprake was van een risicovol contact. Hiermee worden valse positieven zoveel mogelijk beperkt. Als de notificatieapp onvoldoende effectief blijkt, wordt het gebruik ervan beëindigd.

Artikel 8 EVRM

Ingevolge artikel 8, tweede lid, EVRM wordt een inbreuk op de persoonlijke levenssfeer rechtens aanvaardbaar geacht indien deze een legitiem doel dient, de inbreuk bij wet wordt voorzien en de inbreuk noodzakelijk is in een democratische samenleving. In verband met het noodzakelijkheidsvereiste vervullen het dringend maatschappelijk belang en het proportionaliteitsvereiste een belangrijke functie. Het gerechtvaardigd doel van de notificatieapp is voor een belangrijk deel gelegen in de noodzakelijke bescherming van de volksgezondheid. De notificatieapp geeft immers betere controle op besmettingshaarden en de verspreiding van het virus. Daarmee draagt de app ten eerste bij aan de bescherming van de volksgezondheid en ten tweede aan het verder

kunnen afbouwen van de met de intelligente lockdown samenhangende beperkende maatregelen.

De inzet van de notificatieapp maakt zoals toegelicht onderdeel uit van de bron- en contactopsporing van de GGD zoals geregeld in artikel 6, eerste lid, onderdeel c, Wpg. Met de app wordt de GGD ondersteund in de uitvoering van die taak. Daarmee is de inbreuk bij wet voorzien. De bron- en contactopsporing van de GGD is overigens slechts één van de maatregelen die op grond van de Wpg kunnen worden genomen, en daarbij ook één van de lichtere. De Wpg biedt een grondslag om ingrijpende maatregelen in te zetten om infectieziekten te bestrijden, zoals gedwongen isolatie, gedwongen medisch onderzoek en sluiting van gebouwen en terreinen. Het gegeven dat dergelijke maatregelen door de wetgever zijn voorzien, onderstreept de noodzaak van effectieve bestrijding van infectieziekten zoals het virus, in het belang van de volksgezondheid op individueel niveau en de samenleving als geheel. De wetgever heeft daarmee ook bij de totstandkoming van de Wpg al onderkend dat het daartoe gerechtvaardigd is veel van individuen te vragen. Daar staat tegenover dat er voor de inzet van de notificatieapp verschillende belangrijke waarborgen worden getroffen. Allereerst het uitgangspunt, dat het gebruik van de notificatieapp te allen tijde vrijwillig is, zoals ook wordt gewaarborgd door de in het wetsvoorstel opgenomen misbruikbepaling, het feit dat er zo weinig mogelijk gegevens worden verwerkt, gegevens vrijwel niet herleidbaar zijn en zo kort mogelijk worden bewaard. Gelet hierop is de inzet van de notificatieapp proportioneel en daarmee een gerechtvaardigde inbreuk op het recht op de bescherming van de persoonlijke levenssfeer van artikel 8 EVRM.

15. Rechten van de betrokkene



Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

Uitvoering geven aan de rechten van betrokkenen is enkel mogelijk voor een beperkte duur tijdens de validatiefase. Op grond van artikel 11, tweede lid, AVG zijn de verwerkingsverantwoordelijken na verwijdering van de persoonsgegevens (TEKs) die zijn gedeeld met de back-end-server, niet gehouden uitvoering te geven aan artikelen 15 tot en met 20.

Tijdens de overige verwerkingsfasen worden geen persoonsgegevens verwerkt die in de invloedssfeer van de GGD of de minister van VWS liggen. Dit is inherent aan het decentrale en privacyvriendelijke model waarvoor is gekozen.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenoemde gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's



Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

- a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;**
- b. de oorsprong van deze gevolgen;**
- c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;**
- d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.**

In bijlage 1 is een overzicht van risico's opgenomen die een negatief effect op betrokkenen kunnen hebben. Daarbij is, conform de richtlijnen van WP29 voor gegevensbeschermingseffectbeoordelingen, uitgegaan van een intrinsiek risicobegrip. Daarmee wordt bedoeld dat de kans en de impact van de negatieve gebeurtenis beoordeeld worden zonder dat eventuele reeds genomen maatregelen meegenomen worden in de beoordeling. De kans en de impact zijn daarbij kwalitatief ingeschat, met een schaal die van "laag" (L), "middelhoog" (M) naar "hoog" (H) loopt. Daarbij is de schaal van het risico als functie van kans en impact er één van "zeer laag" (LL), "laag" (L), "middelhoog" (M), "hoog" (H) naar "zeer hoog" (HH) loopt.

In Bijlage 1 zijn bij veel gebeurtenissen tevens maatregelen opgenomen. Tevens is er een inschatting gedaan van het restrisico, zijnde het residueel risico onder de aanname dat de beschreven maatregelen volledig geïmplementeerd zijn.

D. Beschrijving voorgenoemde maatregelen

In onderdeel D wordt gezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

17. Maatregelen



Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Er zijn diverse beveiligingsmaatregelen genomen om de beveiliging van de gegevens alsmede de bescherming van de persoonsgegevens te waarborgen:

1. Het kiezen voor een decentrale structuur, waarbij behalve het uitwisselen van sleutels in geval van besmetting alles op de mobiele telefoon gebeurt. Er is geen centrale administratie.
2. Er wordt gewerkt met pseudonieme gegevens, die niet zijn afgeleid van andere gegevens maar volledig willekeurig worden bepaald. Dit betekent dat er geen verborgen herleidbaarheid naar bijvoorbeeld een telefoon is of er een risico bestaat dat de berekening alsnog ongedaan kan worden gemaakt.
3. Infrastructuur
 - a. Op de backend servers worden nog niet gevalideerde gegevens bij de Belastingdienst opgeslagen en niet bij een externe partij. Hierdoor is het mogelijk extra beveiligingslagen te maken, zoals:
 - i. Het scheiden van het IP-adres van de verstuurd data. Hierdoor is het niet mogelijk te herleiden wie welke informatie heeft verstuurd.
 - ii. Er is een scheiding tussen het Security Operations Center en het team aan de back-end, waardoor ook functioneel de TEKS zijn gescheiden van het IP-adres. Het personeel van de verschillende teams kan niet bij elkaars data.
 - iii. Het gebruik van de informatie in het internetprotocol is beperkt tot het absoluut noodzakelijke en er is gekozen voor een korte dataretentie periode.
 - iv. Inzet van het Security Operations Center voor bewaking en monitoring dat beschikt over goede SOPs (Standaard Operating Procedures), waardoor bij incidenten er ook eenduidig en goed handelingsperspectief is. Daarnaast werkt het SOC volgens het 4-eyes principe wat betekent dat er altijd bij handelingen iemand meekijkt om fouten te voorkomen of zeer fors te reduceren.
 - v. Gebruik van een validatiemechanisme om te voorkomen dat
 1. ten onrechte iemand zich met COVID-19 besmet meldt
 2. op het netwerk (van een provider of aanbieder van Wifi) het mogelijk is te herleiden dat iemand besmet is met COVID-19. Dit is mogelijk door af en toe een dummy upload te doen van niet echte sleutels, waardoor netwerkverkeer niet automatisch een besmetting betekent maar ook zinloos verkeer kan zijn.
 - vi. Inzet van het Security Operations Center van de Belastingdienst om actief te monitoren op aanvallen en (ver)storingen. Hierdoor is het mogelijk om snel in te grijpen bij incidenten.
 - vii. Gebruik van standaard schaalbare technologie die hoog beschikbaar is van de Belastingdienst om bij een nieuwe golf van Corona-infecties ook grotere volumes aan uploads probleemloos aan te kunnen.

- viii. Redundantie om bij (ver)storingen te kunnen blijven doordraaien.
 - ix. Gebruik van een HSM voor de sleutels van de cryptografie.
 - b. Inzet van Microsoft Azure Content Delivery Network (CDN) voor sleutels, die mogen worden gedownload. Dit is openbare informatie bestemd voor apps om op te halen. Door het CDN in te zetten, kunnen grote aantallen apps gelijktijdig de gegevens ophalen zonder last hebben. Er zijn de volgende aanvullende maatregelen getroffen:
 - i. Het inzetten van twee datacenters van Microsoft. Zo wordt bij een (ver)storing er een hogere beschikbaarheid gerealiseerd.
 - ii. Monitoring door SOC Belastingdienst om aanvallen of (ver)storingen sneller te detecteren
 - iii. Het gebruik van datacenters binnen de Europese Economische Ruimte om juridische bedreigingen elders ter wereld te pareren
 - iv. Het maken van afspraken in een Service Level Agreement om daarmee te borgen dat een minimaal serviceniveau wordt gehaald
 - v. De inrichting wordt zo gedaan dat de IP-adressen niet worden bewaard. Dit betekent dat via het datacenter niet te achterhalen wie de app heeft geïnstalleerd.
 - vi. De certificaten in de Azure omgeving staan in een vault en kunnen alleen door geautoriseerde medewerkers worden geplaatst.
 - vii. De te delen data mag technisch alleen vanuit het netwerk van de Belastingdienst worden aangeleverd.
 - c. Op de telefoon wordt gebruik gemaakt van de DP3T-implementatie van Apple en Google. Deze laag geeft extra bescherming ten opzichte van het zelf maken, omdat deze is gebouwd met een wantrouwen in de richting van de app. Het protocol is verder state of the art op basis van de laatste wetenschappelijke inzichten.
- 4. Software ontwikkeling. Bij het ontwikkelen van de software zijn er diverse maatregelen getroffen:
 - a. Het ontwerpen op basis van privacy by design
 - b. Het ontwerpen op basis van security by design
 - c. Het ontwikkelen van een cryptografisch raamwerk om versleuteling maximaal en zo effectief mogelijk in te zetten. Dit is een breed plan.
 - d. Het houden aan programmeerstandaarden om zo zogenaamde spaghetti-code te voorkomen en voldoende documentatie te leveren dat de broncode niet aan een of enkele personen hangt om te kunnen onderhouden
 - e. Intensief programma voor hoogwaardige kwaliteit van broncode, waardoor de kans op fouten afneemt, er veiligere software wordt gemaakt dan zonder deze en intensief tijdens de ontwikkeling wordt getest. Dat gebeurt met een aantal stappen:
 - i. Inzet van SonarQube. Dit is een platform dat continue inspectie van de broncode. Hiermee kunnen fouten (bugs),

onderliggende problemen (code smells) en beveiligingszwakheden snel worden gevonden. Deze fouten worden actief tijdens het ontwikkelen gezocht. Daarnaast checkt de software op:

1. het niet houden aan programmeerstandaarden waardoor de app niet onderhoudbaar zou zijn.
 2. gebrekkige uitleg in de code waardoor deze door het volume al snel niet meer te onderhouden is.
 3. verificatie op code die dubbel aanwezig is.
 4. Het uitvoeren van unit tests tijdens de ontwikkeling. Dit betekent dat ieder onderdeel van de software ook los wordt getest van een test over het geheel
- ii. Er is een quality assurance team dat handmatig testen uitvoert op de werking van software.
 - iii. Een ander team voert zogenaamde code reviews uit op de broncode. Dit betekent dat er handmatig wordt gekeken naar de broncode om zo fouten, beveiligingsproblemen en andere problemen op te sporen.
 - iv. Naast de interne slagen is de broncode vrijgegeven als open-sourcesoftware. Dankzij de inzet van een community manager is er een gemeenschap van kritisch meekijkende experts, die aanvullende feedback geven. Hierdoor is er in de fase voor de livegang aanvullende meerwaarde gecreëerd als kwaliteitsslag.
 - v. Er geldt een coordinated vulnerability disclosure om eventuele problemen van derden in ontvangst te nemen.
5. Brede samenwerking en feedbackloops:
- a. Samenwerking in het eHealth netwerk van de Europese Unie om best practices te delen, zoals bijvoorbeeld het coördineren van technische issues, het uitwisselen van DPIA's en risicoinschattingen, coördinatie op het gebied van cryptografie.
 - b. Het hebben van een begeleidingscommissie met onafhankelijke experts, die niet op een andere manier bij het project zijn betrokken (onafhankelijkheid).
6. Interne verificatieslagen. Intern worden een aantal stappen gezet om de kwaliteit en beveiliging van de totale oplossing (app plus backend) te toetsen:
- a. Uitgebreide pentest door pentesters in dienst van de overheid.
 - b. Uitgebreide codereview door overheidsreviewers.
 - c. Intensieve verificatie van configuratie en hardening
7. Externe verificatie. Op weg naar de livegang wordt er een brede inventarisatie gedaan op het gebied van informatiebeveiliging en privacybescherming. De verslaglegging wordt zo maximaal mogelijk openbaar. Hiervoor worden de volgende maatregelen en onderzoeken gedaan:
- a. Het opdelen van de verificatie in veel verschillende percelen, die ieder door een ander bedrijf worden afgetest:
 - i. Hierdoor vindt er een druk tussen de bedrijven plaats, omdat er een dreiging is dat bevindingen over het hoofd worden gezien.

- ii. Verschillende bedrijven hebben andere blikken, waardoor de kans op het maximaal vinden van aandachtspunten wordt vergroot.
 - iii. Meerdere onafhankelijke partijen beïnvloeding lastiger maken, waardoor onafhankelijkheid maximaal is geborgd.
 - iv. Het voorkomen dat een partij 'als vriend van xxx' een rol krijgt en daarmee een vriendendienst regelt.
 - v. Alles wat relatief goed af te testen is ook daadwerkelijk wordt afgetest.
 - vi. Het selecteren van Europese bedrijven met een goede reputatie op het deelgebied waarvoor zij zijn gevraagd offerte uit te brengen.
 - b. Het werken met verschillende percelen voor het uitvoeren van de beveiligingsonderzoeken:
 - i. Uitgebreide penetratietest op de app plus de backend. Gericht op het vinden van fouten.
 - ii. Handmatige codereview van de app gericht op kwaliteit en het waarborgen dat er geen verborgen functionaliteit is of juist functionaliteit ontbreekt.
 - iii. Handmatige codereview op de backend gericht op kwaliteit en het waarborgen dat er geen ongedocumenteerde functionaliteit is of juist functionaliteit achterwege wordt gelaten.
 - iv. Review van de privacyfeatures van de app en de backend, beoordeling van de DPIA.
 - v. Uitvoeren van een analyse op het voldoen aan de BIO door de Belastingdienst.
 - vi. Vergaren van externe analyses en certificeringen van Microsoft voor hun CDN.
 - vii. Verificatie van de instellingen in de backend conform de afspraken.
 - c. Het laten opstellen van een overall review over de onderzoeken om extra waarborgen te creëren dat de beveiliging en privacybescherming maximaal zijn geborgd.
 - d. Een procedurele toelichting over het doorlopen proces
 - e. Het gebruik van de open-sourcecommunity voor feedback
 - f. Het starten van een bugbounty om doorlopend te blijven zoeken naar verbeter mogelijkheden
 - g. Het organiseren van een verified built wat betekent dat een notaris toeziet dat de openbaar gemaakte broncode van de app daadwerkelijk wordt omgezet naar programmatuur en wordt gepubliceerd in de Apple en Google appstore. Van deze actie wordt een verslag gemaakt.
- 8. Risico-analyse. In aanloop naar de testfase heeft er een intensief proces plaatsgevonden om met de inlichtingendiensten, de NCTV en het NCSC om te komen tot een risicoinschatting met bijbehorende mitigatiemaatregelen voor eventuele dreigingen op basis van actoren en te beschermen belangen. Deze maatregelen zijn doorgevoerd bij livegang.

9. Als onderdeel van de dreigingsanalyse wordt regelmatig contact onderhouden met de NCTV, het NCSC en de inlichtingendiensten om veranderingen in het dreigingslandschap snel in maatregelen om te zetten.
10. Bij het verspreiden van de app voeren zowel Apple als Google aanvullende verificatieslagen op de werking van de app uit. Daarmee wordt voorkomen dat de app onbedoelde functionaliteit heeft. Deze worden in de testfase op dezelfde geverifieerd als in de praktijk.
11. Op de portal van de GGD wordt gebruik gemaakt van meerfactorauthenticatie om een verificatiecode te maken.

Zie voor een verdere uitwerking bijlage 1. De (ook in bijlage 1 uitgewerkte) getroffen beveiligingsmaatregelen maken naar het oordeel van VWS dat van een restrisico geen sprake meer is, laat staan van een onacceptabel restrisico.

Bijlage 1: Risico's en Maatregelen

Vragen over nut en noodzaak van een DPIA:

Is er sprake van een grootschalige verwerking? Ja.

Knock-out vragen:

- Worden er bijzondere categorieën van persoonsgegevens verwerkt? Ja. De TEKs zijn bij een upload naar de server in theorie tot een persoon te herleiden. Omdat upload alleen mogelijk is na een positieve uitslag op een COVID-19 test is er sprake van een gezondheidsgegeven.
- Is er sprake van surveillance in de openbare ruimte? Nee.
- Is er sprake van stelselmatig volgen van betrokkenen? Nee. Hier is juist niet sprake van het volgen van betrokkenen. De app is zo gemaakt dat het volgen van betrokkenen niet mogelijk is.
- Is er sprake van kwetsbare groepen? Nee.
- Is duidelijk of de organisatie namens zichzelf verwerkt? Ja.
- Zijn de grondslagen gedocumenteerd? Ja.

Conclusie: Het uitvoeren van DPIA wenselijk en noodzakelijk.

Hoe is de risico-inschatting gemaakt? Er wordt gekeken naar de impact van een risico als dat zou materialiseren en de kans dat dit daadwerkelijk gebeurt. Daarbij wordt een score gemaakt op basis van Laag, Medium, Hoog. De normering is dan als volgt:

Impact

Hoog – De gevolgen voor de betrokkene hebben bij het materialen van het risico forse invloed op het leven van de betrokkene

Middel – De gevolgen voor de betrokkene hebben bij materialiseren van het risico geen beperkte impact op het leven van de betrokkene

Laag – De gevolgen voor de betrokkene hebben materialiseren van het risico weinig of verwaarloosbare invloed op het leven van de betrokkene

Kans

Hoog – Het is zeer waarschijnlijk of zeker dat het risico zal materialiseren

Middel – Het is denkbaar dat dit risico zal materialiseren

Laag – Het is onwaarschijnlijk dat dit risico zal materialiseren

Het risico wordt als volgt samengesteld:

Impact	Kans	Risico
Laag	Laag	Laag-Laag
Laag	Medium	Laag
Laag	Hoog	Medium
Medium	Laag	Laag
Medium	Medium	Medium
Medium	Hoog	Hoog
Hoog	Laag	Medium
Hoog	Medium	Hoog
Hoog	Hoog	Hoog-Hoog

1. Gebruiker onvoldoende specifiek geïnformeerd

Fase: Installatiefase

Categorie: Geïnformeerde vrije keuze

Incident: Te weinig specifiek

Impact: Medium. Als een betrokkene onvoldoende specifiek is geïnformeerd, is het denkbaar dat onaangenaam wordt verrast wanneer een melding op de telefoon wordt gegeneerd.

Kans: Laag. Rond deze app is fors meer informatie beschikbaar dan bij andere apps het geval is. Naast de teksten in de app store, is er veel media aandacht, is er een overheids campagne beschikbaar.

Risico: Laag

Maatregelen:

- Er is onderzoek gedaan naar user-interaction-design om een helder mogelijke interface te maken.
- Er wordt een praktijktest georganiseerd in Twente gericht op de user interface
- Er zijn duidelijk beschrijvingen
- Er komt een duidelijk privacy statement

Beperking/Uitdaging:

Impact na maatregelen: Medium. Als iemand onvoldoende geïnformeerd is dan zal de impact ondanks de maatregelen niet veranderen.

Kans na maatregelen: Laag. De maatregelen zullen al lage risico verlagen.

Risico na maatregelen: Laag

2. Onvrijwillige installatie

Fase: Installatiefase

Categorie: Geïnformeerde vrije keuze

Incident: Niet vrijelijk gegeven

Impact: Laag. Als iemand wordt gedwongen de app te installeren dan zal dat voor de betrokkene als onwenselijk worden ervaren. Het heeft echt geen dermate invloed dat de loop van het leven verandert en het betekent nog niet dat daadwerkelijk informatie wordt verstrekt.

Kans: Laag. Bij installatiefase wordt de app geïnstalleerd en gebeurt niet direct iets met persoonsgegevens. Er wordt een beleid gevoerd rond de vrijwilligheid om te installeren. We laten nadrukkelijk geen mensen onder druk zetten.

Risico: Laag – Laag

Maatregelen:

- Heldere communicatie met betrekking tot de vrijwilligheid van het gebruik van de app
- Aandacht in de media voor de app en de vrijwilligheid ervan
- Er is een Corona wet in de maak, die een zware sanctie zet op dwang (half jaar cel, 8.000 euro boete)

Beperking/Uitdaging:

Google weigert bepaalde teksten in het besturingssysteem aan te passen, waardoor onduidelijk kan ontstaan rond de API.

– Weigering OS-makers bepaalde teksten besturingssysteem aan te passen (Google)

Impact na maatregelen: Laag. Impact verandert niet.

Kans na maatregelen: Laag. De kans wordt kleiner indien de maatregelen worden genomen.

Risico na maatregelen: Laag-Laag

3. Geblokkeerde app in de store

Fase: Installatie

Categorie: Middelen

Incident: Een app is geblokkeerd in de store. Derden gebruiken (automatische/juridische) takedown processen om te app tijdelijk opgeschort te laten worden in de app-store, bijvoorbeeld door een oneigenlijke auteursrechtelijke claim in te dienen.

Impact: Medium. Een betrokkene verwacht te worden gewaarschuwd en kan van de dienst geen gebruik maken. Dat zal leiden tot ongemak.

Kans: Laag. Gelet op het mogelijk afbreukrisico (schadeclaim) is de kans niet groot dat dit snel zal gebeuren.

Risico: Laag.

Maatregelen:

- Afspraken maken met Google/Apple dat er geen geautomatiseerde take-down zal zijn
- Piketdienst om op verstoringen als deze snel te acteren
- Follow-beleid om de schade te verhalen. Bij auteursrechtenclaims betaalt de partij die ongelijk krijgt alle noodzakelijke kosten

Beperking/Uitdaging:

Impact na maatregelen: Medium. Impact verandert niet.

Kans na maatregelen: Laag.

Risico na maatregelen: Laag

4. Replay van RPI's

Fase: Uitwisselingsfase

Categorie: Gegevens

Incident: Met een replay aanval worden opnames gemaakt van uitgezonden (al dan niet via de ether) data om deze op een later moment nogmaals uit te zenden. Hierdoor wordt een verwerking nogmaals gedaan door eenzelfde of een ander systeem. RPIs kunnen op deze manier worden opgenomen en vervolgens opnieuw worden uitgezonden. Hierdoor lijkt het alsof iemand vlakbij is geweest. Er kunnen bij zo'n aanval ten onrechte RPI's worden verwerkt. Het probleem daarbij ontstaat op het moment dat er een RPI tussen zit die gecorrigeerd is met iemand die in het recente verleden of de nabije toekomst bekend staat/komt als een COVID-19-besmetting.

Een aanval is lastig om op grote schaal te doen, het kan eigenlijk alleen realistisch in een klein gebied met een beperkt aantal telefoons.

Impact: Medium. Wanneer een RPI wordt uitgezonden die later blijkt te behoren bij een persoon die positief test op COVID-19 dan is het mogelijk dat er een melding door de app wordt gegenereerd. De betrokkene zou in dat geval een advies kunnen krijgen een test te doen. Dat is een onprettige ervaring, maar niet een die het leven blijvend op de kop zal zetten.

Kans: Laag. Het is heel moeilijk om een dergelijke aanval met succes uit voeren, waarbij het resultaat ook is dat iemand een melding krijgt. Het uitvoeren op grote schaal zonder ontdekking is ingewikkeld. Daarbij is het risico beperkt tot het 15 minuten tijdsframe voor er een nieuwe RPI wordt aangemaakt.

Risico: Laag.

Maatregelen:

- Er is redelijke bescherming van de integriteit van het bericht
- Opvolging op basis van het verwerkingsverbod onder de AVG (een onbevoegde mag geen gezondheidsgegevens verwerken);
- Betrokkene wijzen op de mogelijkheid om de overtreder aansprakelijk te stellen en een schadevergoeding te eisen op basis van artikel 82 AVG. Dit beleid actief te communiceren.
- Opvolging op basis van computervredebreuk en het toevoegen van gegevens aan een geautomatiseerd werk (138ab/350a Sr.) De ervaring leert dat zowel de strafeis als de strafoplegging forse hoger zijn bij Corona-aso's.

Beperking/Uitdaging: Grote (institutionele) partijen (winkelcentra, NS, Schiphol, Ziggo/etc) kunnen in grote gebieden luisteren c.q. hun infrastructuur kan gehijacked worden omdat te doen. In dat laatste geval is er wel sprake van een beveiligingsincident van nationale omvang.

Impact na maatregelen: Medium. Impact zou niet veranderen.

Kans na maatregelen: Laag.

Risico na maatregelen: Laag.

5. Gemanipuleerde RPI's via relay

Fase: Uitwisselingsfase

Categorie: Gegevens

Incident: Bij een relay aanval wordt data op een bepaald punt opgevangen om deze op een andere locatie weer uit te zenden. Op deze manier worden bijvoorbeeld auto's gestolen. Het is denkbaar dat een dergelijke aanval wordt uitgevoerd op een locatie waar een hoge besmetting wordt verwacht. Dit is bijvoorbeeld bij een GGD-teststraat. Daarbij moet wel worden bedacht dat moment ongeveer 0,7% van de tests positief is, waardoor zelfs daar het succes beperkt zal zijn.

Omdat het hier RPI's betreft, moet het signaal vrijwel direct worden uitgezonden omdat deze binnen 15 minuten vervangen worden. Een aanvaller dient ook tenminste vijf minuten onopgemerkt per telefoon met sterk signaal te ontvangen om succes te hebben, omdat anders het contact niet wordt geregistreerd als potentieel risicovol.

De werking van de aanval impliceert dat moet samen worden gewerkt, die vervolgens moet proberen meerdere telefoons te bereiken om enig succes te hebben. Het is technisch mogelijk, maar zeer bewerkelijk. Dit probleem is van wetenschappelijke onderbouwing voorzien in de Mind the GAP-analyse²³.

Impact: Medium. Wanneer een RPI wordt uitgezonden die later blijkt te behoren bij een persoon die positief test op COVID-19 dan is het mogelijk dat er een melding door de app wordt gegenereerd. De betrokkene zou in dat geval een advies kunnen krijgen een test te doen. Dat is een onprettige ervaring, maar niet het leven blijvend op de kop zetten.

Kans: Laag. Het is zeer bewerkelijk om uit te voeren, waarbij de kans op succes relatief laag is.

Risico: Laag.

Maatregelen:

- De RPI's wisselen om de 15 minuten en moeten binnen die tijd worden uitgezonden.
- Opvolging op basis van het verwerkingsverbod onder de AVG (een onbevoegde mag geen gezondheidsgegevens verwerken);
- Betrokkene wijzen op de mogelijkheid om de overtreder aansprakelijk te stellen en een schadevergoeding te eisen op basis van artikel 82 AVG. Dit beleid actief te communiceren.
- Opvolging op basis van computervredebreuk en het toevoegen van gegevens aan een geautomatiseerd werk (138ab/350a Sr.). De ervaring leert dat zowel de strafeis als de strafoplegging forse hoger zijn bij Corona-aso's.

Beperking/Uitdaging:

Impact na maatregelen: Medium. De impact verandert door de maatregelen niet.

Kans na maatregelen: Laag.

Risico na maatregelen: Laag.

²³

<https://arxiv.org/pdf/2006.05914.pdf>

6. Denial of Service

Fase: Uitwisselingsfase

Categorie: Gegevens

Incident: Uitzenden extreme volumes snel wisselende RPIs, zal notificatie-app in klein gebied effectief onbruikbaar maken.

Impact: Medium. Een gebruiker zou in een geval waar deze tijdens de aanval in contact staat met iemand die later positief test voor COVID-19 zou een terechte notificatie kunnen missen.

Kans: Laag. Het is een behoorlijk specifieke aanval, die gedurende langere tijd op dezelfde telefoons moet worden uitgevoerd om succesvol te zijn.

Risico: Laag.

Maatregelen:

- De RPI's wisselen om de 15 minuten en moeten binnen die tijd worden uitgezonden.
- Opvolging op basis van computervredebreek en het ontoegankelijk maken van gegevens van een geautomatiseerd werk (138ab/350a Sr.). De ervaring leert dat zowel de strafeis als de strafoplegging forse hoger zijn bij Corona-aso's.

Beperking/Uitdaging: Het risico speelt in de API-laag van Apple en Google, waardoor er afhankelijkheid is van technische maatregelen die deze bedrijven nemen. Welke dat zijn is onduidelijk. Daarom leunen we alleen op organisatorische maatregelen.

Impact na maatregelen: Medium. De impact verandert niet.

Kans na maatregelen: Laag.

Risico na maatregelen: Laag.

7. Onbevoegde tracking

Fase: Uitwisselingsfase

Categorie: Omgeving

Incident: Het is mogelijk dat personen digitaal worden gevolgd. De traceerbaarheid van personen is mogelijk over periodes van 15 minuten, omdat daarna de RPI verandert. Indien er een buitengewoon klein aantal mensen in het gebied onder observatie is, bestaat de mogelijkheid om een redelijk beeld te krijgen over die 15 minuten heen. Daarbij moet worden opgemerkt dat het eenvoudiger is om 'reguliere' wifitracking uit te voeren.

Impact: Laag. De tracking heeft geen directe impact op de personen, omdat de partijen die dit doen niet kunnen herleiden naar een persoon.

Kans: Laag. Gelet op de wettelijke verboden is de kans klein dat dit op enige schaal zal gebeuren.

Risico: Laag-Laag

Maatregelen:

- Opvolging op basis van het verwerkingsverbod onder de AVG (een onbevoegde mag geen gezondheidsgegevens verwerken);
- Betrokkene wijzen op de mogelijkheid om de overtreder aansprakelijk te stellen en een schadevergoeding te eisen op basis van artikel 82 AVG. Dit beleid actief te communiceren.
- Actieve opvolging op basis van in ieder geval overtreding van in ieder geval 350a Sr. en waar mogelijk andere wetsartikelen. De ervaring leert dat zowel de strafeis als de strafoplegging forse hoger zijn bij Corona-aso's.

Beperking/Uitdaging: Het is een fundamentele eigenschap van het protocol om Bluetooth-signalen te kunnen opvangen en RPI's uit te wisselen. Het zou hier onbevoegd gebruik betreffen.

Impact na maatregelen: Laag. Het inzetten van de gegevens is dermate onaantrekkelijk dat een geavanceerde aanval met dit doel niet logisch is.

Kans na maatregelen: Laag

Risico na maatregelen: Laag-Laag

8. Reconstructie van gangen van mobiele telefoons

Fase: Uitwisseling

Categorie: Omgeving

Incident: Een partij met een inrichting met veel systemen en antennes gericht op het afvangen van signalen in grote gebieden zou de gangen van een persoon in dat gebied kunnen nagaan als deze persoon zijn of haar besmetting publiceert. Dit komt omdat de RPI's na publicatie zijn te herleiden.

Impact: Middel. Er zou onrechtmatig een patroon van een COVID-19-besmette betrokkene worden gemaakt. Deze zou daar tijdelijk overlast van kunnen ondervinden door onheuse bejegening onrechtmatig weigeren van toegang.

Kans: Laag. Om een dergelijke aanval moet er sprake zijn een grote partij die deze aanval uitvoert of een criminele organisatie van veel samenwerkende partijen. De aanval is louter gericht op een COVID-19 geïnfecteerde met een app. Voor het volgen van mensen door grote organisaties is het waarschijnlijker dat er gebruik wordt gemaakt van wifi of bluetooth tracking in plaats van het implementeren van DP3T-protocol.

Risico: Laag.

Maatregelen: Het is een fundamentele eigenschap van het protocol om Bluetooth-signalen te kunnen opvangen en RPI's uit te wisselen. Het zou hier onbevoegd gebruik betreffen. Wanneer de infrastructuur van een grote partij wordt overgenomen om te misbruiken voor dit risico dan zou er sprake zijn van een informatiebeveiligingsincident met uitstraling van het bedreigen van de nationale veiligheid).

Beperking/Uitdaging:

Impact na maatregelen: Laag. Om deze gegevens te misbruiken moet een geavanceerde aanval worden uitgevoerd met een enorm afbreukrisico.

Kans na maatregelen: Laag.

Risico na maatregelen: Laag-Laag

9. Depseudonimisatie

Fase: Uitwisselingsfase

Categorie: Omgeving

Incident: Bij het zeer stelselmatig onrechtmatig observeren (bijvoorbeeld onrechtmatige observatie door een burger, OV-chipkaartpoortje, check-in bij gebouw) zou het mogelijk zijn dat op basis van een gepubliceerde melding het toch mogelijk is een betrokkene te identificeren. Dit probleem is van wetenschappelijke onderbouwing voorzien in de Mind the GAP-analyse²⁴.

Impact: Middel. Iemand krijgt onrechtmatig te weten dat een persoon met COVID-19 besmet is. Het is denkbaar dat op basis van deze informatie een onrechtmatige daad zou worden gepleegd (bijvoorbeeld het weigeren van een persoon op een locatie).

Kans: Laag. Het is voor een enkele partij zeer arbeidsintensief om de informatie bij te houden en te koppelen. Voor grote partijen is het onwaarschijnlijk om dat het verboden is en er snellere methoden zijn om een COVID-19-besmetting in kaart te brengen. Denk bijvoorbeeld aan het meten van de temperatuur van een bezoeker. Iets wat her en der in de praktijk ook gebeurt.

Risico: Laag.

Maatregelen:

- Het regelmatig wisselen van de RPI
- Opvolging op basis van het verwerkingsverbod onder de AVG (een onbevoegde mag geen gezondheidsgegevens verwerken);
- Betrokkene wijzen op de mogelijkheid om de overtreder aansprakelijk te stellen en een schadevergoeding te eisen op basis van artikel 82 AVG. Dit beleid actief te communiceren.
- Opvolging op basis van computervredebreuk en het toevoegen van gegevens aan een geautomatiseerd werk (138ab/350a Sr.). De ervaring leert dat zowel de strafeis als de strafoplegging forse hoger zijn bij Corona-aso's.

Beperking/Uitdaging:

Impact na maatregelen: Laag. Het gebruiken van de informatie die eventueel wordt verkregen, introduceert voor de dader een risico op problemen op basis van aansprakelijkheid, AVG en het strafrecht.

Kans na maatregelen: Laag.

Risico na maatregelen: Laag-Laag

²⁴

<https://arxiv.org/pdf/2006.05914.pdf>

10. Justitie of inlichtingendiensten verschaffen zich toegang tot telefoon

Fase: Uitwisselingsfase

Categorie: Omgeving

Incident: OM of veiligheids- en inlichtingendiensten van Nederland of een land waar de betrokkene zich bevindt verschaffen zich toegang tot RPIs of TEKs van telefoon door hier fysiek toe te krijgen en de API-laag van Google/Apple te kraken.

Impact: Hoog. De informatie kan in de verkeerde context leiden tot negatieve beeldvorming of tegen de persoon worden ingezet.

Kans: Laag. De telefoon bewaart alleen de laatste twee weken en dat er daadwerkelijk toegang is tot iemands telefoon is klein. Het is waarschijnlijker dat langs andere weg dezelfde informatie sneller en effectiever wordt verkregen. En daarbij kunnen OM of inlichtingendiensten alleen onder de daarvoor in wet- en regelgeving gestelde voorwaarden, en met inachtneming van de daarin voorziene waarborgen en beperkingen, zich daartoe toegang verschaffen.

Risico: Medium.

Maatregelen:

- Er staat een verzoek uit bij het Parket Generaal en de AIVD om zeer terughoudend om te gaan met de informatie van de COVID-19-notificatieapp. Dit is momenteel in beraad.
- Google en Apple hebben versleuteling aangebracht, die eerst moet worden gekraakt alvorens de toegang succesvol is.
- Google en Apple maken geen cloud backups van de DP3T-gegevens. Hierdoor is deze informatie niet langs andere weg te krijgen. Er moet fysieke toegang tot de telefoon zijn.
- De API is zo ingericht dat andere apps dan de Rijksoverheid app er niet bij kunnen. Daarnaast is de inrichting volgens het model dat Google/Apple de derde partij (onze app) standaard wantrouwend benaderen

Beperking/Uitdaging:

Impact na maatregelen: Laag. Als er afspraken komen dan is de data off limits en zal dan ook niet snel te gebruiken zijn.

Kans na maatregelen: Laag.

Risico na maatregelen: Laag-Laag

11. API of andere apps slaan RPI's te lang op

Fase: Uitwisselingsfase

Categorie: Gegevens

Incident: Het API of een andere app van de mobiele telefoon bewaren RPI's langer dan de afgesproken 14 dagen. Dit zou kunnen gebeuren door een fout in de software.

Impact: Laag. Er wordt geen informatie zomaar buiten de telefoon gebracht. De ouderdom van een contact speelt een rol bij het tonen van een besmettingsmelding en daarmee is de kans op extra false positives heel laag.

Kans: Laag. Dit is afgetest en wordt gecontroleerd.

Risico: Laag – Laag

Maatregelen: Wordt door de API van Apple/Google geblokkeerd

Beperking/Uitdaging:

Impact na maatregelen: Laag

Kans na maatregelen: Laag

Risico na maatregelen: Laag-Laag

12. Derden slaan RPI's te lang op

Fase: Uitwisselingsfase

Categorie: Gegevens

Incident: Derden slaan RPI's te lang op

Impact: Laag. Er wordt geen informatie zomaar buiten de telefoon gebracht. De ouderdom van een contact speelt een rol bij het tonen van een besmettingsmelding en daarmee is de kans op extra false positives heel laag.

Kans: Laag. De Google/Apple API slaat informatie niet langer op en blokkeert onrechtmatige apps voor gebruik. Reguliere DP3T apps in andere landen voldoen aan dezelfde standaarden.

Risico: Laag-Laag

Maatregelen: Wordt door API onmogelijk gemaakt

Beperking/Uitdaging:

Impact na maatregelen: Laag

Kans na maatregelen: Laag

Risico na maatregelen: Laag-Laag

13. Besturingssysteem of andere apps zien TEKs

Fase: Uitwisselingsfase

Categorie: Gegevens

Incident: Een andere app of het besturingssysteem ziet de TEKs op de mobiele telefoon heeft toegang tot TEKs.

Impact: Laag. Toegang door een andere app of het besturingssysteem op zichzelf maakt geen onrechtmatige verwerking of leidt niet tot het lekken van informatie, zolang de data binnen hetzelfde geautomatiseerde werk (de mobiele telefoon) blijft.

Kans: Laag. De API van Apple/Google is gemaakt om juist deze data te beschermen en weg te houden bij het OS of andere apps. Per land is er maar een app die toegang mag hebben tot deze data.

Risico: Laag-Laag

Maatregelen: De Google/Apple API-laag blokkeert de informatie voor andere apps en het eigen besturingssysteem.

Beperking/Uitdaging:

Impact na maatregelen: Laag

Kans na maatregelen: Laag

Risico na maatregelen: Laag-Laag

14. Wetenschappers verzamelen TEKs

Fase: Uitwisselingsfase

Categorie: Gegevens

Incident: Wetenschappers verzamelen grote aantallen TEKs over zeer lange periodes op. Op grote schaal worden deze verwerkt en bestudeerd. De huidige cryptographische technieken volgens E-Crypt/ENISA zijn geschikt, maar gaan wel uit van een korte levensduur van de TEKs. Het is waarschijnlijk niet bestand tegen wetenschappelijk onderzoek dat zeer langdurig (bijvoorbeeld meer dan 50 jaar).

Impact: Laag. Er is geen directe herleidbaarheid naar de persoon. Het meest waarschijnlijk is dat dit in een labomgeving zal gebeuren. Daar waar daadwerkelijke gegevens worden gebruikt, is de inbreuk zeer beperkt. Over 50 jaar zal het niet interessant zijn welke burger met wie in verbinding stond.

Kans: Hoog. Het is zeer waarschijnlijk dat er veel wetenschappelijk onderzoek zal volgen op de Corona-crisis. Dat het wetenschappelijke DP3T-protocol daarmee onderwerp van onderzoek zal worden, is waarschijnlijk. Over er voldoende geld komt voor een dergelijk langlopend onderzoek en dit langs een ethische commissie zal komen, is zeer twijfelachtig.

Risico: Medium

Maatregelen: Cryptografie geschikt volgens EU normen voor 50 jaar

Beperking/Uitdaging: Alle cryptografie is afhankelijk van een random number generator. Het is onduidelijk hoe goed deze over de tijd zal blijken voor mobiele devices.

Impact na maatregelen: Laag.

Kans na maatregelen: Hoog.

Risico na maatregelen: Medium.

15. Menselijke fouten bij vrijgeven code

Fase: Validatiefase

Categorie: Mensen

Incident: Fout bij vrijgeven code. Een medewerker van de GGD voert een code voor vrijgave verkeerd in (al dan niet bewust) bijvoorbeeld bij een verkeerde persoon. Hierdoor zal een upload van sleutels niet leiden tot publicatie. Tot de medewerkers behoren ook callcenter medewerkers die worden ingehuurd en minder bedreven zijn met de GGD-processen en daardoor sneller fouten maken.

Impact: Medium. Er worden sleutels geüpload, die niet doorvloeien om te worden verspreid. Hierdoor is het mogelijk dat er bij betrokkene informatie niet doorkomt, waardoor zij geen notificatie krijgen waar dat wel wenselijk is. De impact zal effect hebben bij nieuwe haarden bij Corona-uitbraken. Het is redelijk te verwachten dat er dan meer contacten zijn, die leiden tot een melding. Voor de betrokkene persoonlijk is de impact beperkt, omdat het beleid en advies momenteel is om bij de minste klachten een test te ondergaan.

Kans: Medium. De kans op fouten zal toenemen als de druk op de teststraten toeneemt en er meer mensen positief worden bevonden. Bij een tweede golf van Corona-uitbraak zal de druk op medewerkers toenemen.

Risico: Laag.

Maatregelen:

- Opleiding GGD-medewerkers, in validatieproces directe terugkoppeling aan GGD-medewerkers over juistheid code geven.
- Ontwikkelen van een vriendelijke gebruikersinterface die leidt tot minder fouten.

Beperking/Uitdaging:

Impact na maatregelen: Laag. De kans op fouten neemt fors af tot een enkel incident.

Kans na maatregelen: Laag

Risico na maatregelen: Laag-Laag

16. Gebruiker drukt op upload knop zonder besmetting

Fase: Validatiefase

Categorie: Mensen

Incident: Een gebruiker drukt op de upload knop zonder dat er een bevestigde besmetting is. Dit kan per ongeluk gebeuren of omdat iemand dat 'leuk' vindt.

Impact: Laag. Er vindt wel een upload plaats, maar dat zal niet leiden tot publicatie. Bij de backend-server wordt er pas gepubliceerd als de sleutels zijn vrijgegeven door de GGD. Indien deze sleutel niet tijdig komt dan worden de bestanden vernietigd. De upload zal geen resultaat hebben die voor andere betrokkenen merkbaar is.

Kans: Medium. Het is waarschijnlijk dat dit weleens zal worden geprobeerd.

Risico: Laag.

Maatregelen:

- Voorlichting over de werking van het bevestigingsmechanisme met impliciete boodschap dat spelen zinloos.
- Besef van gebruikers dat de app bedoeld is om de corona uitbraken in te dammen en proberen te verstoren asociaal is.

Beperking/Uitdaging:

Impact na maatregelen: Laag.

Kans na maatregelen: Laag.

Risico na maatregelen: Laag-Laag

17. Gebruiker onvoldoende specifiek geïnformeerd

Fase: Validatiefase

Categorie: Geïnformeerde vrije keuze

Incident: Een gebruiker is onvoldoende **geïnformeerd** dat het uploaden van sleutels vrijwillig is of is niet specifiek genoeg **geïnformeerd**.

Impact: Medium. Het uploaden betekent niet dat iemand herleidbaar wordt, omdat daar veel maatregelen tegen zijn getroffen en de pseudonimisatie cryptografisch goed geborgd is. Er is dan ook geen directe impact voor de betrokkene in kwestie. Wel is het zeer onprettig om een upload en later te realiseren dat men dat eigenlijk niet heeft gewild. Tot slot is de toestemming die hier wordt beschreven niet een toestemming op basis van de AVG. Het is een extra waarborg om mensen na een besmetting bewust te laten delen.

Kans: Laag. De kans dat dit onvoldoende **geïnformeerd** gebeurd is niet hoog, omdat er veel wordt gecommuniceerd dat het gebruik van de app en het uploaden van de sleutels op basis van vrijwilligheid gebeurt. Er is veel informatie beschikbaar over de werking van de app, zoals bijvoorbeeld de infographic.

Risico: Laag

Maatregelen:

- Actieve communicatie, marketing campagne
- Infographic
- Duidelijke teksten in de app
- Het testen van de user interface
- Uitleg in opleiding aan zorgverlener hoe de betrokkene te informeren

Beperking/Uitdaging: Onduidelijke artikelen in de media die leiden tot misverstanden, apps in andere landen die anders functioneren (bijvoorbeeld China, Singapore, Noorwegen, etc.)

Impact na maatregelen: Medium.

Kans na maatregelen: Laag

Risico na maatregelen: Laag

18. Upload onder druk

Fase: Validatiefase

Categorie: Geïnformeerde vrije keuze

Incident: Een betrokkene ervaart dat er onwenselijke druk wordt uitgeoefend om de eigen sleutels te uploaden.

Impact: Medium. Het uploaden betekent niet dat iemand herleidbaar wordt, omdat daar veel maatregelen tegen zijn getroffen en de pseudonimisatie cryptografisch goed geborgd is. Er is dan ook geen directe impact voor de betrokkene in kwestie. Wel is het zeer onprettig om een upload tegen zijn of haar zin in. Tot slot is de toestemming die hier wordt beschreven niet een toestemming op basis van de AVG. Het is een extra waarborg om mensen na een besmetting bewust te laten delen.

Kans: Medium. Het is begrijpelijk dat de omgeving van een met COVID-19 besmet persoon (familieleden of vrienden) druk uitoefenen om de upload van sleutels te doen uit oogpunt van maatschappelijk belang. Alleen het verschil tussen overtuigen en druk uitoefenen die de vrije wil te boven gaat, is een dunne lijn. Het is niet onwaarschijnlijk dat dit weleens zal gebeuren.

Verder is het denkbaar dat een zorgverlener iets te veel nadruk legt op het uploaden van sleutels, waardoor dit als onwenselijke druk wordt ervaren.

Risico: Medium.

Maatregelen:

- Zorgverlener opleiden om geen druk uit te oefenen
- Heldere communicatie dat gebruik en upload vrijwillig zijn

Beperking/Uitdaging:

Impact na maatregelen: Medium

Kans na maatregelen: Laag.

Risico na maatregelen: Laag.

19. Backend niet beschikbaar

Fase: Validatiefase

Categorie: Middelen

Incident: De backend is geheel of gedeeltelijk door een (ver)storing langdurig (vele uren of dagen) niet beschikbaar, waardoor het niet mogelijk is om sleutels te uploaden en/of te ontvangen.

Impact: Hoog. Er zijn drie mogelijke gevolgen denkbaar:

- Als er geen sleutels kunnen worden geüpload zouden deze verloren kunnen gaan, zodat ook niet op een later moment worden verstuurd.
- De GGD zou niet in zijn om sleutels te voorzien van een autorisatiecode, waardoor deze bij zeer langdurige storingen niet meer tijdig aankomen en er oudere uploads worden verwijderd.
- Als het niet mogelijk is om een download te doen, komen deze niet bij de app. Het gevolg is dat het mogelijk is dat een notificatie niet wordt gegenereerd waar dat wel had moeten.

In samenhang bezien is de hele functionaliteit van de app dan effectief niet meer beschikbaar.

Kans: Laag. De keuze in technologie is dermate van aard dat de kans klein is. Zowel het datacenter van de Belastingdienst als het Content Delivery Network van Microsoft kennen een hoge beschikbaarheid.

Risico: Medium.

Maatregelen:

- Actieve monitoring van de omgeving door het inzetten van het Security Operations Center van de Belastingdienst zorgt dat een verstoring snel te detecteren. Zij kunnen vlot met de juiste experts schakelen om snel in te grijpen bij een verstoring.
- Er wordt gewerkt met redundantie op verschillende plaatsen:
 - Voor het Content Delivery Network voor het downloaden van de publiek beschikbare lijsten wordt gewerkt met twee datacenters van Microsoft in twee verschillende landen.
 - Voor het uploaden van sleutels wordt gebruik gemaakt van de technologie, die de Belastingdienst ook voor de belastingaangiftestraat gebruikt.
 - Er wordt gewerkt met de anti-DDOS-maatregelen en DDOS-procedures van het Belastingdienst Security Operations Center voor de upload en validatiesleutels. Voor het Content Delivery Network van Microsoft heeft het bedrijf eigen anti-DdoS-voorzieningen.
- Het hebben van een helder afgesproken Service Level Agreement moet waarborgen dat verstoringen kort van aard zijn.
- Intensieve kwaliteitsborging. Om de kans op verschillende vormen van misconfiguratie of softwarefouten tegen te gaan, wordt een kwaliteitsbeleid gevoerd. Dit bestaat onder andere uit (voor zowel de app als de backend):
 - Geautomatiseerde kwaliteitschecks op broncode
 - Het uitvoeren van unit tests op de broncode
 - Handmatige code audits
 - Het uitvoeren van diverse intensieve penetratietesten
 - Het als open-sourcesoftware vrijgeven van de software met actief community management (het werven van vrijwillige experts) voor brede peer review
 - Tijdens het ontwikkelen worden unit tests uitgevoerd. Dit betekent dat ieder onderdeel van de software ook los wordt getest
 - Coordinated vulnerability disclosure om eventuele problemen van derden in ontvangst te nemen.
- Bij het verzenden van sleutels wordt een zogenaamde queue aangemaakt. Een kortere verstoring leidt dan niet tot het verloren gaan van de informatie.

Beperking/Uitdaging:

Impact na maatregelen: Medium. Door de vele maatregelen op functieherstel bij een (ver)storing zal er snel informatie verloren gaan. Ook zullen in verreweg de meeste situaties snel herstel van de functionaliteit zijn.

Kans na maatregelen: Laag.

Risico na maatregelen: Laag.

20. Collision TEKs

Fase: Validatiefase

Categorie: Middelen

Incident: Omdat er wordt gewerkt met willekeurig gekozen TEKs (om daarmee de anonimiteit van de betrokkenen te borgen) is het mogelijk dat er in een gelijke periode van 14 dagen op verschillende telefoons dezelfde TEK wordt aangemaakt. Theoretisch gaat dan om twee of zelfs meer telefoons. Een dergelijk duplicaat dat in hetzelfde systeem optreedt noemen we in de technologie een collision.

Als een van de eigenaren van de telefoons positief test op COVID-19 en de sleutels uploadt dan worden deze gepubliceerd. Door de dubbele TEKs zullen niet mensen met contact met de besmette persoon een notificatie krijgen, maar ook de mensen die in contact stonden met de niet-besmette persoon/personen.

Anders dan bij toeval zou het ook denkbaar zijn dat iemand een aanval uitvoert om willekeurige TEKs uit te zenden.

Impact: Medium. In een ongelukkige situatie krijgt een grotere groep mensen een notificatie waar dat niet zou moeten. Wanneer het ook een persoon betreft met dubbele TEKs die veel contacten heeft (door bijvoorbeeld veel in het openbaar vervoer te zitten).

Kans: Laag. Om op te treden moet de collision binnen dezelfde periode van 14 dagen optreden. De kans is astronomisch laag, omdat hiervoor een 256-bit TEKs wordt gebruikt. Er zijn dan ook 2 tot de macht 256 ofwel

115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.665.640.564.039.457.584.007.913.129.639.936 TEKs mogelijk. Daarbij moet de collision optreden in het Nederlandse netwerk (of in later stadium in het buitenland met een telefoon dat in contact met een Nederlandse telefoon).

Risico: Laag.

Maatregelen:

Beperking/Uitdaging: Het is moeilijk een maatregel tegen te nemen.

Impact na maatregelen: Medium.

Kans na maatregelen: Laag.

Risico na maatregelen: Laag.

21. Nep-backend

Fase: Validatiefase

Categorie: Middelen

Incident: Het internetverkeer wordt omgeleid naar een nep-backend.

Impact: Hoog. Er wordt een valse omgeving gecreëerd en dat zou de mogelijkheid openen om betrokkenen op verschillende manieren te kunnen misleiden, valse informatie te sturen of op andere manieren proberen ellende uit te halen. Een dergelijke aanval zou direct veel mensen betreffen.

Kans: Laag. Het is een aanval die veronderstelt dat onopgemerkt een aanval op de omgeving wordt uitgevoerd, waarbij ook het pinned PKI-Overheidscertificaat wordt nagemaakt.

Risico: Medium.

Maatregelen:

- Actieve monitoring door het Belastingdienst SOC
- Uitvoeren diverse tests, waaronder meerdere penetratietesten

Beperking/Uitdaging:

Impact na maatregelen: Hoog.

Kans na maatregelen: Laag.

Risico na maatregelen: Medium.

22. Backend op netwerk geblokkeerd

Fase: Validatiefase

Categorie: Middelen

Incident: Doordat er wordt gewerkt met een pinned PKI-overheidscertificaat zullen sommige bedrijfsnetwerken het netwerkverkeer met de backend blokkeren. Dat komt door sommige firewalls al het netwerkverkeer willen analyseren. Deze firewalls willen de versleuteling ongedaan maken om de inspectie uit te voeren (een man in the middle aanval).

Het pinned PKI-overheidscertificaat maakt die controle onmogelijk en dat verkeer zal worden geweigerd.

Impact: Laag. Er vindt geen uitwisseling met het netwerk plaats. Gebruikers die alleen via Wifi-netwerken data met een dergelijke firewall uitwisselen zullen hier hinder van ondervinden. Zij kunnen via een ander netwerk of via het mobiele netwerk de data alsnog uitwisselen.

Kans: Laag. Dit zal bij een klein percentage gebruikers daadwerkelijk tot problemen leiden.

Risico: Laag-Laag

Maatregelen: Ander netwerk gebruiken

Beperking/Uitdaging: Deze beperking is in het ontwerp onvermijdelijk, omdat het wel inspecteerbaar maken van het netwerkverkeer zou leiden tot een dreiging tot de privacy. De minister heeft expliciet aangegeven dat herleidbaarheid tot een absoluut minimum moet worden beperkt (de privacy is gewaarborgd).

Impact na maatregelen: Laag

Kans na maatregelen: Laag

Risico na maatregelen: Laag-Laag

23. Datalekken

Fase: Validatiefase

Categorie: Gegevens

Incident: In validatiefase zijn de TEKs tijdelijk minder pseudoniem en op labcode 'gegroepeerd' in de tijdelijke/interne database.

Impact: Medium. Bij een succesvolle aanval kunnen de gegevens van een beperkte TEKs worden gevonden. Het is daarmee niet direct mogelijk de personen te achterhalen. In combinatie met een andere aanval zou het wel mogelijk kunnen zijn om te achterhalen wie positief is getest op COVID-19.

Kans: Laag. Er wordt stevig ingezet op beveiliging en de kans op een succesvolle aanval is klein.

Risico: Laag.

Maatregelen:

- Actieve monitoring
- Intensieve kwaliteitsborging. Om de kans op verschillende vormen van misconfiguratie of softwarefouten tegen te gaan, wordt een kwaliteitsbeleid gevoerd. Dit bestaat onder andere uit (voor zowel de app als de backend):
 - Geautomatiseerde kwaliteitschecks op broncode
 - Het uitvoeren van unit tests op de broncode
 - Handmatige code audits
 - Het uitvoeren van diverse intensieve penetratietesten
 - Het als open-sourcesoftware vrijgeven van de software met actief community management (het werven van vrijwillige experts) voor brede peer review
 - Tijdens het ontwikkelen worden unit tests uitgevoerd. Dit betekent dat ieder onderdeel van de software ook los wordt getest
 - Coordinated vulnerability disclosure om eventuele problemen van derden in ontvangst te nemen.

Beperking/Uitdaging:

Impact na maatregelen: Medium.

Kans na maatregelen: Laag.

Risico na maatregelen: Laag.

24. Toegang door OM/Politie of inlichtingendiensten

Fase: Validatiefase

Categorie: Gegevens

Incident: Via een vordering van het OM, een inbeslagname door de politie of ingrijpen van een inlichtingendienst valt een mobiele telefoon in handen van deze instanties. Zij kunnen in theorie bij de TEKs komen als zij de beveiliging van Apple/Google doorbreken.

Impact: Hoog. Als de data wordt gebruikt om in te zetten tegen een betrokkene dan kan dat verstrekkinge gevolgen hebben voor deze persoon.

Kans: Laag. De kans dat de API van Google/Apple te kraken is en dat een mobiele telefoon in handen van de partijen op een moment dat ze relevante data bevat is klein door de 14-dagen retentieperiode. Het is daarnaast ook een kleine kans. Voor een succesvolle aanval moet toegang zijn tot de mobiele telefoon. Vergelijkbare informatie is sneller te vergaren door vorderingen bij de operator en clouddienstverleners. Zij beschikken immers over meer informatie die door mobiele telefoons worden gegenereerd dan deze app.

Risico: Medium.

Maatregelen:

- Sterke versleuteling om daarmee de kans op succes van het benaderen van de gegevens te verkleinen
- Retentie. Door gegevens na twee weken weg te gooien is de kans op het bestaan van nuttige informatie fors verminderd
- In het nationaal belang vragen om deze data off limits te verklaren voor informatie op de mobiele telefoon en de infrastructuur. Dit ook om weerstand bij gebruik weg te nemen. Dit uit oogpunt dat het bestrijden van COVID-19 een groter belang is dan het belang van een individueel onderzoek en het ondermijnen van het vertrouwen van het systeem.
- Het uitvoeren van onderzoek op de cryptografie.

Beperking/Uitdaging: Zowel de inlichtingendiensten als het Parket Generaal hebben aangegeven niet open staan voor het off limits verklaren van de app.

Impact na maatregelen: Laag. Bij het off-limits verklaren van deze data verdwijnt de impact.

Kans na maatregelen: Laag.

Risico na maatregelen: Laag-Laag

25. Belastingdienst verschaft toegang tot TEKs

Fase: Validatiefase

Categorie: Gegevens

Incident: Door een aanval uit te voeren verschaft de Belastingdienst zich toegang tot de TEKs tegen afspraken in.

Impact: Medium. Het gaat hier om TEKs die kort daarna publiek gemaakt worden. In combinatie met andere gegevens is er herleidbaarheid denkbaar in sommige gevallen. Het is onduidelijk wel nut hiermee gediend zou worden.

Kans: Laag. Het is zeer onwaarschijnlijk dat dit wordt gedaan, gelet op alle beheersmaatregelen

Risico: Laag.

Maatregelen:

- Splitsing tussen SOC en beheer van de backend
- Governance
- Afspraken in de verwerkersovereenkomst

Beperking/Uitdaging:

Impact na maatregelen: Medium

Kans na maatregelen: Laag

Risico na maatregelen: Laag

26. Verkeersanalyse

Fase: Validatiefase

Categorie: Transmissie

Incident: Door verkeersgegevens te analyseren zou een netwerkbeheerder kunnen achterhalen wie er TEKs ophalen naar de Belastingdienst. Daaruit zou de conclusie te trekken zijn dat deze personen positief zijn getest op Corona. Dit zou bij een telecomoperator kunnen gebeuren, maar ook bij een bedrijf door bijvoorbeeld het Wifi-netwerk in de gaten te houden.

Impact: Medium. De herleidbaarheid zou kunnen leiden tot tijdelijke maatregelen.

Bijvoorbeeld een werkgever die personeel naar huis stuurt.

Kans: Medium. Het is denkbaar dat bepaalde beheerders dit gaan doen.

Risico: Medium.

Maatregelen:

- Door ook netwerkverkeer te genereren met dummy-data zegt een upload niets meer. Iedere telefoon zal af en toe updates genereren. Er is een grotere kans dat iemand niet besmet is dan wel. Wie netwerkverkeer in de gaten houdt ziet alleen versleutelde data langskomen. Bij de backend wordt het dummy-verkeer nooit gevalideerd en daarmee vernietigd.
- Onrechtmatige verwerking op basis van de AVG, die operators en beheerders van wifinetwerken niet mogen uitvoeren.

Beperking/Uitdaging:

Impact na maatregelen: Medium

Kans na maatregelen: Laag. Het is zeer onwaarschijnlijk dat met succes een aanval wordt uitgevoerd om duidelijk te krijgen of iemand besmet is.

Risico na maatregelen: Laag

27. Derden bewaren TEKs te lang

Fase: Validatiefase

Categorie: Middelen

Incident: Derden bewaren TEKs langer dan 14 dagen.

Impact: Laag. Het is moeilijk de TEKs aan een betrokkene te koppelen

Kans: Hoog. Het is zeer waarschijnlijk dat derden dit zullen proberen.

Risico: Medium.

Maatregelen:

- Opvolging op basis van het verwerkingsverbod onder de AVG (een onbevoegde mag geen gezondheidsgegevens verwerken).
- Betrokkene wijzen op de mogelijkheid om de overtreder aansprakelijk te stellen en een schadevergoeding te eisen op basis van artikel 82 AVG. Dit beleid actief te communiceren.

Beperking/Uitdaging:

Impact na maatregelen: Laag.

Kans na maatregelen: Medium.

Risico na maatregelen: Laag.

28. Derden analyseren publieke TEKs

Fase: Validatefase

Categorie: Middelen

Incident: Derden downloaden de publieke lijsten voor analyse met eigen lijsten. Dat kan zowel nationaal als over meerdere landen worden gedaan.

Impact: Laag. Vergelijken is dezelfde functionaliteit als die de app levert. Het blijven zeer moeilijk herleidbare pseudoniemen.

Kans: Hoog. Het zal zeer waarschijnlijk geprobeerd worden.

Risico: Medium

Maatregelen:

- Opvolging op basis van het verwerkingsverbod onder de AVG (een onbevoegde mag geen gezondheidsgegevens verwerken).
- Betrokkene wijzen op de mogelijkheid om de overtreder aansprakelijk te stellen en een schadevergoeding te eisen op basis van artikel 82 AVG. Dit beleid actief te communiceren.

Beperking/Uitdaging:

Impact na maatregelen: Laag

Kans na maatregelen: Medium

Risico na maatregelen: Laag

29. Herintroductie oude TEKs

Fase: Validatefase

Categorie: Middelen

Incident: Door een fout worden oude gepubliceerde TEKs nog eens geïntroduceerd. Een ander scenario door een dubbele upload.

Impact: Laag. De kans is astronomisch klein dat dezelfde TEKs nogmaals zal leiden tot een waarschuwing bij een persoon.

Kans: Laag. Bij de publicatie is er geen verwerking anders dan het beschikbaar stellen van de informatie aan de publicatieservers voor download door derden. Bij een moedwillige aanval vereist het vervalsen van 2x PKI overheid certificaat handtekening (het vervalsen van een unmanaged EC/DSA key pair is -niet- nodig; want deze heeft geen datum).

Risico: Laag-Laag

Maatregelen:

- Maatregelen van behoorlijk beheer.
- Monitoring door SOC

Beperking/Uitdaging:

Impact na maatregelen: Laag

Kans na maatregelen: Medium

Risico na maatregelen: Laag

30. App raakt corrupt

Fase: Notificatiefase

Categorie: Middelen

Incident: De app of de mobiel raakt beschadigd of corrupt waardoor deze niet meer functioneert.

Impact: Medium. Er zullen geen notificaties worden gemaakt.

Kans: Laag. Zal niet snel gebeuren

Risico: Laag.

Maatregelen:

- Herinstallatie door gebruiker

Beperking/Uitdaging:

Impact na maatregelen: Medium

Kans na maatregelen: Laag

Risico na maatregelen: Laag

31. Screenshot notificatie

Fase: Notificatiefase

Categorie: Middelen

Incident: Gebruiker maakt screenshot van "risico op besmet"-melding, voordat hij of zij deze wegklikt. Het screenshot wordt gebruikt om als 'bewijs' te gebruiken bij werkgever of school. Dit wordt bij voldoende voorkomen iets wat 'verwacht' wordt. Problemen voor participatie of dwang om toch de app te installeren al kiest de gebruiker hier zelf voor.

Impact: Middel. Problemen voor participatie of dwang om toch de app te installeren al kiest de gebruiker hier zelf voor.

Kans: Medium.

Risico: Medium.

Maatregelen:

- Heldere communicatie met betrekking tot de vrijwilligheid van het gebruik van de app
- Aandacht in de media voor de app en de vrijwilligheid ervan
- Er wordt gewerkt aan een wetsvoorstel waarin het direct of indirect verplicht gebruik van de app expliciet wordt verboden

Beperking/Uitdaging:

Impact na maatregelen: Medium

Kans na maatregelen: Laag

Risico na maatregelen: Laag

32. Omkeerbaarheid RPI's of TEKs

Fase: Niet fasegebonden

Categorie: Middelen

Incident: De bestaande cryptografie wordt op zo'n manier doorbroken dat deze de RPI's of TEKs berekenbaar maakt.

Impact: Medium. In de uitwerking zou dat betekenen dat bij een grote hoeveelheid punten waar TEKs worden ontvangen en opgeslagen iemand te volgen zou zijn. Omdat wordt gewerkt met willekeurige nummers in plaats van waarden die naar een toestel te herleiden zijn, is misbruik erg lastig. Daarvoor zou een observatie infrastructuur moeten worden gemaakt. De relatie tussen een TEK en een RPI is ook gemaakt op basis van hashing, waardoor de cryptografie een kant op werkt (je kunt niet ontcijferen).

Kans: Laag. Er wordt gebruik gemaakt van sterke cryptografie. Er is door het Europees agentschap ENISA een evaluatie uitgevoerd op robuustheid van de gekozen cryptographische algoritmes.

Risico: Laag.

Maatregelen:

- Borging op de Europees niveau

Beperking/Uitdaging:

Impact na maatregelen: Medium

Kans na maatregelen: Laag

Risico na maatregelen: Laag

