

Feitenrelaas inzake gebeurtenissen omtrent coronatest-IT-systeem van de GGD

- Voor onderstaand feitenrelaas zijn onder andere Kamercorrespondentie, Kamerstukken en notulen van overleggen geraadpleegd waar deze thematiek is besproken. De geraadpleegde documenten zijn uit de periode januari 2020 – januari 2021.
- In dit feitenrelaas is gepoogd zo volledig mogelijk te zijn. Gezien het korte tijdsbestek, kan niet worden uitgesloten dat er nog meer stukken beschikbaar komen die relevant zijn. Deze stukken worden dan zo spoedig mogelijk gedeeld met de Kamer.

April / mei 2020

- **De Tweede Kamer wordt geïnformeerd** over het opzetten van nieuwe IT-systemen om o.a. het proces van aanvraag tot terugkoppeling uitslag test en het BCO te automatiseren en vergemakkelijken (kamerstukken: 25295-277; 25295-315).
- In de Kamerbrief van 6 mei wordt de *Taskforce digitale ondersteuning bestrijding COVID-19* aangekondigd (kamerstuk 25295-315).
- In de brief van 19 mei wordt gemeld (kamerstuk 25295-317): *“de voorbereidingen van de IT-applicatie CoronIT lopen op schema. Hierbij wordt voldaan aan de eisen van veilig gebruik van gegevens van burgers.”*

Juni 2020

- **4 juni voortgangsbrief (Kamerstuk 25295-386):**
“Ik heb een wetsvoorstel in voorbereiding om misbruik van de app [voor BCO] door derden te verbieden, waarbij ik ook van de gelegenheid gebruik maak om expliciet in de Wpg vast te leggen dat de GGD-en bij het bron- en contactonderzoek gebruik kunnen maken van digitale ondersteuning zoals de app.”
- **24 juni stand van zakenbrief (Kamerstuk 25295-428):**
In verschillende passages wordt melding gemaakt dat er wordt gewerkt aan het optimaliseren van de keten, onder meer door de koppelingen van IT-systemen: *“Ook werken RIVM en GGD aan verbetering van de registratiesystemen zodat op landelijk niveau een goed en betrouwbaar inzicht te geven is in de verspreiding en indamming van het virus.”*

Juli 2020

- **15 juli: Bericht AD “Storing in coronadatabase:** gegevens kwijt over kinderen en zorgverleners”
 - o *“Door een storing in de database waarin informatie over geteste coronapatiënten wordt opgeslagen, waren belangrijke gegevens van het bron- en contactonderzoek kwijt. Zo was onduidelijk hoeveel kinderen, zorgverleners en leraren afgelopen week besmet raakten.”*
 - o *“Oorzaak van het probleem is volgens het RIVM de database van CoronIT, het speciaal voor corona opgerichte IT-systeem waarin kenmerken worden opgeslagen van positief geteste coronapatiënten. Van vorige week maandag tot afgelopen zondag zijn er 73.000 mensen getest. Van den Hof [hoofd van het Centrum voor Epidemiologie en Surveillance van Infectieziekten]: „De database is zo groot geworden, dat het problemen geeft. Het gaat om de testuitslagen en gegevens van 370.000 mensen, getest sinds 1 juni. Dat aantal neemt nog steeds toe, die database is gigantisch groot.”*
- **Op 16 juli wordt in de Kamerbrief (kamerstuk 25259-460)** de lancering van de CoronaMelder gemeld. Later in deze maand (kamerstuk 25295-466):
“Op dit moment zet de GGD-GHOR ook in op een verdere verbetering van CoronIT, het systeem dat uitwisseling van testgegevens tussen GGD'en en laboratoria ondersteunt. Deze verbeteringen zullen leiden tot een beter en meer gedetailleerd beeld van de doorlooptijden. Knelpunten die ontstaan kunnen dan ook sneller en preciezer worden geïdentificeerd en opgelost. [...] Ook wordt nu snel meer capaciteit vrijgemaakt om de testuitslagen door te bellen en de GGD-GHOR bouwt op dit moment een digitaal portaal waar mensen met (bij COVID-19 passende) klachten via een beveiligde omgeving (DigID) een afspraak kunnen inplannen voor een testafpraak. Indien de uitslag negatief is, zal deze ook via hetzelfde portaal worden teruggegeven. Dit tweede, digitale kanaal zal halverwege augustus live gaan en zal de druk afnemen van het callcenter en een positief effect hebben op de doorlooptijden.”
- **Op 16 juli publiceert de IGJ** een toezichtskader Testen en bron- en contactonderzoek. Daarin staat onder andere:

- "Medewerkers in de testlocatie beschikken over materialen voor afname en toegang tot CoronIT."
- En: "Alle medewerkers van het BCO hebben toegang tot HPZone en zijn opgeleid om registratie in het programma op de juiste manier uit te voeren."

Augustus 2020

- **6 augustus Kamerbrief ontwikkelingen COVID-19 (kamerstuk 25295-469):**
"Vanaf 1 september is het ondersteunende ICT-systeem voor deze testketen (CoronIT) verder verbeterd waardoor een heel precies beeld ontstaat over de doorlooptijden per fase en de knelpunten die er landelijke én lokaal ontstaan. En dat maakt gericht ingrijpen dan ook mogelijk. Vervolgens is het de verwachting dat door het live gaan van het digitaal portaal op 12 augustus (waar je met je DigID zelf een afspraak kan maken en je eigen testuitslag ook zelf weer kunt inzien) de doorlooptijden verder verbeteren."

September 2020

- **16 september: Nieuwsuur bericht** over 'Testlijnmedewerkers kunnen bij persoonsgegevens, ook als dat niet mag'. In dit artikel licht GGD toe:
"Volgens de GGD kunnen alle callcentermedewerkers bij alle dossiers omdat ze de informatie van mensen die bellen voor een afspraak moeten kunnen controleren. De GGD controleert naar eigen zeggen scherp wie wat doet in het systeem. Medewerkers moeten aangeven welk dossier ze hebben geopend. Wie de geheimhouding schendt door zonder reden in dossiers te kijken, kan worden opgespoord. De GGD kan (nog) niet zeggen of en hoe vaak dat is voorgekomen."
- **17 september: Twee sets Kamervragen (2020Z16523 en 2020Z16515)**
ontvangen van de leden Ellemeet, Smeulders en Buitenweg (GL) en Hijink (SP) naar aanleiding van berichtgeving van Nieuwsuur over 'Testlijnmedewerkers kunnen bij persoonsgegevens, ook als dat niet mag' van 16 september.
- **Op 17 september publiceert de IGJ** het eerste toezichtsrapport over de keten van testen en traceren. Daarin schrijft de Inspectie: *"Ook keek de inspectie naar de twee ICT-systemen: CoronIT voor het registreren van de testafspraken en uitslagen en HPZone voor het registreren van het bron- en contactonderzoek. Gaandeweg het onderzoek zag de inspectie hier steeds meer stabiliteit en koppelingen ontstaan waardoor de knelpunten op ICT-gebied steeds minder werden."*
- **18 september: Notulen 'Stuurgroep 'Oplossing 2 (IZB) app' [Voorloper Stuurgroep GGD Contact].**
 - Stand van zaken omtrent de realisatie van 'Oplossing 2' [voorloper GGD Contact] wordt besproken:
 - *"Nieuwe versie van het PvA opgestuurd. Volgende versie wordt dit uitgebreid met stukken over de go live planning, bedreigingsanalyse en user stories."*
 - *"Vanuit de taskforce gedrag is naar voren gekomen dat er een grote groep gebruikers is die juist meer data met de GGD'en wilt delen. Belangrijk om dit scenario mee te nemen in de verdere ontwikkeling van de app."*
 - *"Komende week staat de informatiebeveiliging (IB) op de planning om hier verdere invulling aan te geven. VWS meldt dat het dreigingsniveau van de toekomstige applicatie hoog is. [...] Dit is van invloed op de IB van de app maar ook op de gekoppelde systemen van de GGD. Noodzakelijk om snel duidelijkheid te verkrijgen op de gevolgen voor Oplossing 2 hiervan."*

Oktober 2020

- **5 oktober: Opdrachtbrief Voorzitter Stuurgroep LCT.**
Van de minister van VWS krijgt de heer Van der Zande de opdracht om per direct het voorzitterschap van de Landelijke Coördinatiestructuur Testcapaciteit (LCT) te vervullen. *"In deze fase van de crisis is er behoefte aan een steviger governance op de testketen en een duidelijke regie op de samenwerking."*
- **16 oktober: Notulen 'Stuurgroep 'Oplossing 2 (IZB) app'**
 - Hierin wordt het voorstel besproken om *"één portaal te ontwikkelen waarmee het gehele BCO-proces wordt ondersteund"*. Verschillende GGD'en hebben zich aangemeld voor een praktijktest. De stuurgroep stemt met dit voorstel in.
 - Omtrent functionaliteit eerste versie Oplossing 2 wordt vermeld *"dat de exacte impact op het gebied van informatiebeveiliging (IB) en privacy nog onduidelijk is. VWS stemt toe dit met het programma RDO [Realisatie Digitale Ondersteuning] verder te onderzoeken"*.
- **30 oktober: Notulen 'Stuurgroep 'Oplossing 2 (IZB) app'**

- De "Gevolgen voor privacy en informatiebeveiliging in kaart brengen t.a.v. uitbreiden functionaliteit Oplossing 2", worden besproken.
- "Er is twee weken geleden een notitie naar de stuurgroep gegaan ter besluitneming om te onderzoeken of de functionaliteit van Oplossing 2 kan worden uitgebreid met het informeren van de contacten door de index zelf d.m.v. de app. Besluit is genomen onder voorbehoud van Privacy en politieke overwegingen. Uit onderzoek van VWS is gebleken dat hier risico's op het gebied van informatiebeveiliging en privacy zijn. Daarom wordt er nu gekeken naar een andere invulling op deze functionaliteit waar, i.p.v. gebruik te maken van de app, er via een beveiligde mailservers contacten een bericht ontvangen. Uitgangspunt hierin is dat dit bericht geen medische gegevens mag bevatten. Er wordt in dit bericht gevraagd om in te loggen op een beveiligde omgeving waarin dit wel mogelijk is."
- Een van de onderwerpen die zich op "het kritische pad" bevindt, is de DPIA (Data protection impact assessment); "de DPIA is niet gereed op 30 oktober. Deze moet wel beschikbaar zijn voordat de praktijktesten gaan beginnen."

November 2020

- 2 november: PO GGD GHOR –VWS

Het "Proces ICT-infrastructuur RIVM, GGD GHOR, VWS" wordt besproken. "Het gesprek over de ICT-infrastructuur is gestart en de escalatielijns is duidelijk." Ook komt er een structureel regieoverleg waarin de inhoudslijns en de ICT-lijns worden besproken.

- 3 november: bericht in het AD "GGD-medewerkers gluurden ongeoorloofd naar BN'ers in coronadatabase":

"Het datalek kwam aan het licht nadat een tipgever via het anonieme klokkenluidersplatform Publeaks melding deed van misbruik van de enorme database van de GGD. „Via de Database van CoronIT, waar de resultaten van coronatesten worden geregistreerd, kan iedereen gegevens opzoeken van allerlei mensen, bekenden en invloedrijke Nederlanders."

- 4 november: in het debat over de ontwikkeling rondom het coronavirus stelt het lid Kuzu (DENK) vragen over de beveiliging van persoonsgegevens (en lichaamsmateriaal) in de testketen. De minister antwoordt dat hier tal van wettelijke voorwaarden aan verbonden zijn en zegt toe hier in een brief nader op in te gaan [dit gebeurt in de brief van 8 december, Kamerstuk 25295-771].

- In de eerste helft november blijkt wordt in het LCT (Landelijke Coördinatiestructuur Testcapaciteit) gesignaleerd dat er specifieke aandacht moet worden gegeven aan IT onder regie van het de LCT. Op welke manier dit moet gebeuren is onderwerp van gesprek is de overleggen van 5 en 12 november 2020. Er wordt dan nog gesproken over een "Werkgroep raamwerk IT".

- 5 november verslag PO Testen en Traceren VWS – GGD GHOR

- "GGD GHOR is hard bezig met het uitbreiden en verbeteren van CoronIT. De inzet is om hierin niet te hoeven prioriteren."
- "GGD GHOR geeft aan dat het invoeren van asymptomatisch testen invloed zou kunnen hebben op CoronIT."

- 9 november verslag PO VWS – GGD GHOR

- Gemeld wordt dat er digitale ondersteuning komt bij HP-Zone. Dit helpt BCO-medewerkers om sneller te registreren. Ook wordt gemeld dat De app 'Oplossing 2' voor tijdswinst lijkt te kunnen gaan zorgen bij het BCO. De eerste pilot is geweest in West-Brabant, en dat ziet er veelbelovend uit.
- Over "concept oplevering data infrastructuur" wordt het volgende gezegd: "Vorige week donderdag is er gestart met een architectuurplaat van het ICT-landschap. Hier is een team mee bezig. Er wordt gekeken naar de afhankelijkheden en de kwetsbaarheden. Aanstaande vrijdag wordt een eerste concept verwacht, waarschijnlijk met aanbevelingen. GGD GHOR geeft aan dat ze het belangrijk vinden om de communicatie af te stemmen, en om de opdracht aan een rapportage van PA-consulting gezamenlijk op te pakken. VWS stemt hiermee in."

- 10 november: Notulen 'Stuurgroep 'Oplossing 2 (IZB) app'

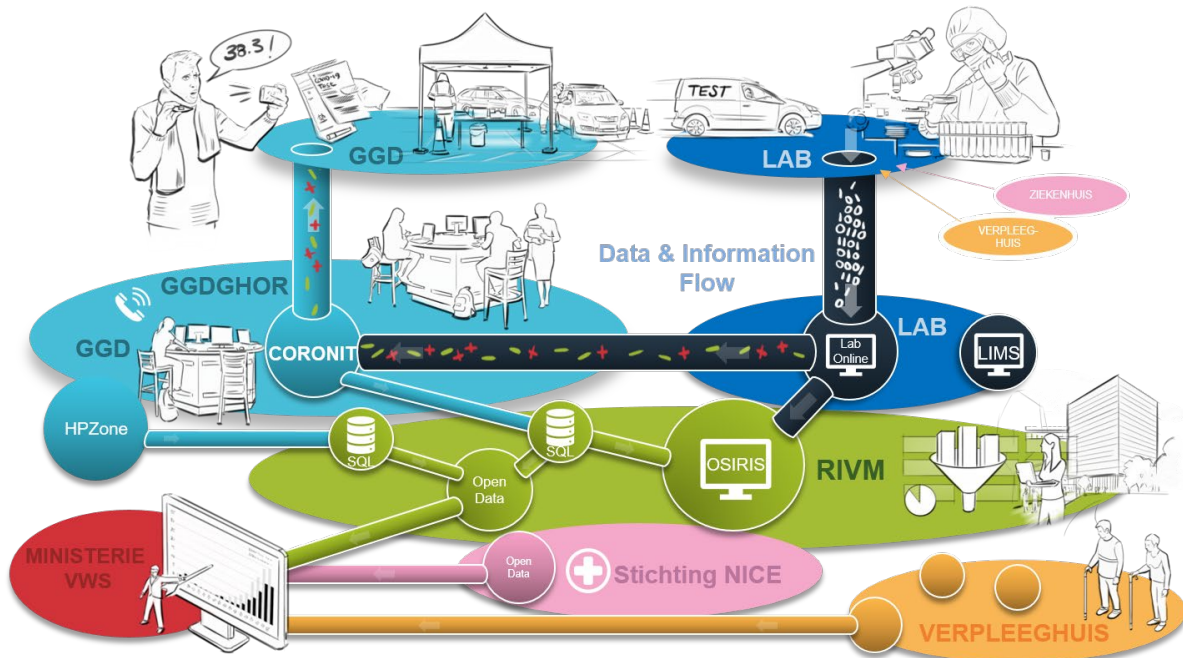
Bij agendapunt "Mail functionaliteit om de index te ondersteunen", licht VWS toe dat "is vastgesteld dat het informeren van contacten via de app als functionaliteit niet geschikt is bevonden op het gebied van informatiebeveiliging (IB) en privacy. Er is nu een voorstel ontwikkeld om de contacten van de index te informeren d.m.v. veilige email. Hierin zijn de IB en privacy problemen wel te overkomen maar deze uitwerking is op het

gebied van gebruiksvriendelijkheid misschien minder effectief. Hier wordt nog aan gewerkt."

- **13 november: Notulen 'Stuurgroep 'Oplossing 2 (IZB) app'**
De governance van de stuurgroep wordt besproken.
- **13 november: Bestuur overleg MVWS – DPG'en**
Besproken wordt dat *digitale oplossingen zoals HPZone Lite en Oplossing 2 BCO effectiever maken*".
- **16 november: Verslag PO VWS – GGDGHOR**
In het PO verslag van 16 november staat onderstaande, voor de leesbaarheid is dit enigszins geparafraseerd:
 - o "GGD GHOR heeft van de voorzitter van het LCT begrepen dat er resultaten zijn van een quick scan van de IT-systemen, maar heeft daar zelf nog niets van vernomen, dit terwijl zij vorige week uitdrukkelijk had afgesproken met VWS hier gezamenlijk op te sturen. Toen was het ook al mis gegaan.
 - o GGD GHOR verzoekt VWS om intern te zorgen dat duidelijk is dat er gezamenlijk wordt gestuurd en dus de resultaten te delen, te bespreken en gezamenlijk conclusies uit te trekken en afgestemde communicatie voor te bereiden.
 - o Actie: VWS geeft aan hierover contact op te nemen met collega's binnen VWS, nog voor het verschijnen van de kamerbrief.
 - o GGD GHOR geeft aan dat er waarschijnlijk twee verschillende initiatieven zijn, naast de quickscan ook een analyse gericht op de toekomstbestendigheid van de verschillende IT-systemen.
 - o GGD GHOR geeft aan dat zij ook bij dit initiatief betrokken wil zijn, om gezamenlijk opdrachtgever te zijn. Het gaat immers om systemen van de GGD/GHOR.
 - o Actie: VWS stuurt uitkomsten eerste analyse toekomstbestendigheid naar GGD GHOR."
- **17 november: stand van zakenbrief COVID-19**
 - o De Kamer wordt geïnformeerd over de ontwikkeling van GGD Contact [hiervoor naar verwezen als: 'Oplossing 2 app']: "Deze digitale oplossing ondersteunt de GGD bij het uitvoeren van bron- en contactonderzoek door het verzamelen en registreren van gegevens te versnellen en vereenvoudigen."
 - o Over GGD Contact: "Net als bij de ontwikkeling van CoronaMelder worden daaraan [privacy, gegevensbescherming en informatieveiligheid] ook nu geen concessies gedaan. Gelet op de gevoeligheid van de verwerkte gegevens worden extra maatregelen genomen op het gebied van informatiebeveiliging."
 - o "Gedurende het realisatieproces van GGD Contact wordt, tot slot, opnieuw kritisch meegekeken en geadviseerd door de Taskforce Digitale Ondersteuning bestrijding COVID-19 en de Taskforce Gedragwetenschappen."
- **17 november: beantwoording Kamervragen GL en SP (Kamerstukken 2020D46582 en 2020D46581)**
 - o "Omdat niet kan worden voorspelt wie er een bepaalde dag belt voor het maken van een afspraak, moeten alle callcentermedewerkers bij alle dossiers kunnen"
 - o "De privacy van de betrokkenen is dan ook goed gewaarborgd en er zijn de nodige checks & balances ingeregeld in de werkprocessen. Zo is er bijvoorbeeld een scherpe controle op de logging. Door zorgvuldig te loggen wordt nauwlettend bijgehouden welke dossiers door wie worden ingezien."
 - o "Als blijkt dat er regels worden overtreden, worden er maatregelen genomen."
- **18 november: technische briefing aan de vaste commissie voor Volksgezondheid, Welzijn en Sport** door André van der Zande, voorzitter Landelijke Coördinatiestructuur Testcapaciteit
 - o Uit de presentatie:
 - o "Dan de testketen zelf. Dat is toch best nog een ingewikkeld ding. Je kunt het heel eenvoudig beschrijven. Dan zeg je dat het gaat om het maken van een afspraak, het afnemen op een bepaalde plek, waar dan ook, het verwerken, waarvoor met monsters door het land gereden wordt – u ziet daar ook autootjes bij staan – tussen teststraten en laboratoria, de analyse en de rapportage door het laboratorium en de verantwoording vanuit de testuitslag naar de burger, het RIVM en het ministerie, dus de partijen die het moeten weten. Naast monsters gaat er over die testketen dus ook een hele hoop informatie. Daar zitten ook kwetsbaarheden in en we zijn op dit moment bezig om die te verbeteren."
 - o "Dan de IT-systemen. We hebben te maken met zeven verschillende IT-systemen. Die zijn natuurlijk dedicated voor de taak waar ze voor bedoeld zijn."

Denkt u aan HP Zone of CoronIT of OSIRIS, waar ik zelf goed mee bekend ben vanuit mijn RIVM-verleden. Dat zijn de IT-systemen waar we mee werken, maar die moeten natuurlijk met elkaar praten en dat moet een doorlopende stroom zijn.”

- o Gepresenteerde plaat van de testketen:



- o Uit de vragenronde:
- o **Mevrouw Agema (PVV):** "Tijdens het afnemen van de swap, de test, wordt het burgerservice-nummer gevraagd van degene die zich laat testen. Waarom gebeurt dat? Welke informatie wordt daaraan gekoppeld? Hoelang wordt dat gegeven bewaard? Wat is precies de gang van zaken rondom dat bsn?"
De heer Van der Zande: De hele keten is gebaseerd op de privacyvereisten die gelden voor de samenleving. Voor gericht medisch onderzoek zijn er uitzonderingen mogelijk. Het wordt in nauw overleg met de autoriteit bekeken. Dat gebeurt ook bij nieuwe introducties in de ICT-infrastructuur of bij een app. Het bsn is nodig om terug te kunnen melden aan degene bij wie de swap is afgenomen: u bent positief of u bent negatief. Er is ook een koppeling met de medische dossiers. Of het zonder burgerservicenummer zou kunnen, weet ik niet. Dat zouden we moeten uitzoeken. Op dit moment vindt de identificatie plaats via het burgerservicenummer.
De voorzitter: Hoelang wordt het bewaard?
De heer Van der Zande: Weet ik niet. Dat zou ik moeten opzoeken."
- o **De heer Öztürk (DENK):** "Voorzitter. Testen is vrijwillig, maar de testbereid is niet zo hoog. Een groep mensen twijfelt en vindt het hele testen niet transparant: wat gebeurt er met de gegevens van de burgers? Zo werd er net terecht een vraag gesteld over het burgerservicenummer. Maar wordt er ook DNA van burgers afgenomen? Worden de testresultaten ergens opgeslagen? Heel veel burgers hebben daar twijfels en vragen over. Kunt u een lijst geven met wat er precies in alle stappen gebeurt met het testen, waar de gegevens heen gaan, wie die opslaat en hoelang die worden opgeslagen? Hoe kan er uiteindelijk transparantie komen, zodat burgers weten wat er met hun gegevens wordt gedaan?"
De heer Van der Zande: Dat kan ik nu niet zeggen, maar we kunnen het wel laten uitzoeken. Over het DNA-materiaal staat er volgens mij een passage in de brief met de termijnen waarin dat bewaard en weggegooid wordt. Maar heel gedetailleerd van elke stap aangeven waar de data zitten, kan ik op dit moment niet. Dat zou wel uitgezocht kunnen worden. We zouden daar een memo of iets dergelijks over kunnen opstellen." [dit gebeurt in de brief van 24 december, Kamerstuk 25295-843]

- **18 november: Motie lid Kuzu (nr. 735)**, hierin wordt de regering verzocht om te bewerkstelligen dat mensen duidelijk voorgelicht worden over wat er met hun lichaamsmaterialen en DNA kan gebeuren na het afnemen van een coronatest.
- **26 november: Verslag PO VWS – GGD GHOR**

De planning van ICT en het vervolg wordt besproken:

- o *"Er is een risicoanalyse gedaan waar quick wins uit zijn gekomen.*
- o *In de kamerbrief die 8 december naar de Kamer gaat willen we iets zeggen over waar we mee bezig zijn op gebied van ICT. De incidenten [met betrekking tot instabiliteit van datasystemen] blijven voortbestaan, het is belangrijk om de Kamer te informeren.*
- o *Volgende week is er contact tussen VWS en GGD over de kamerbrief, bespreken wat we in de kamerbrief zetten. 9 december is er weer een regulier coronadebat.*
- o *GGD GHOR vraagt zich af waar de regiegroep onder wordt gehangen. Dit wordt vanmiddag ook in het LCT besproken. Goed communiceren over wat er al wel kan, zoals het webportal."*
- **27 november: in de 'Stuurgroep GGD Contact' (nieuwe naam van 'Stuurgroep 'Oplossing 2 (IZB) app')** wordt gesproken over de planning lancering en communicatie van GGD Contact. In de presentatie worden ook de onderwerpen bijgehouden *"die zich op het kritieke pad bevinden"*:
 - o *"De referentie DPIA [Data protection impact assessment] en het accorderen van de FG'en [functionarissen gegevensbescherming] van de DPIA. Om dit gereed te krijgen is de schatting nu dat er twee extra weken nodig zijn. Hiervoor is ook de landsadvocaat ingeschakeld om bij het opstellen te helpen. Het is nog onduidelijk hoe snel de DPIA precies gereed kan zijn."*

December 2020

- **1 december: eerste bijeenkomst Regiegroep Digitale Ondersteuning Test- en Traceerketen (DOTT)**
 - o *Uit verslag 1 december: "Aanleidingen voor oprichting van de Regiegroep is: 1. Instabiliteit van (overgang tussen) informatiesystemen en 2. Reguleren van een stroom initiatieven die betrekking hebben op de test- en traceerketen (o.a. apps)." De regiegroep rapporteert aan LCT.*
 - o *De stand van zaken van de risicoanalyse wordt besproken: [De risicoanalyse] "Is in uitvoering. Gesprekken tussen RIVM, GGD en VWS verlopen goed en de opdracht is er. Er wordt gekeken naar storingen en acties die daaruit voortvloeien, de focus is de technische mankementen en afhankelijkheden. M.b.t. proces: a.s. vrijdag was niet haalbaar. De resultaten worden op 11 december opgeleverd en kunnen worden gecombineerd met de risicoanalyse GGD (uitgevoerd door KPMG) die op 18 december wordt verwacht. Er wordt, t.b.v. communicatie, gekeken naar een integrale set van informatie met aanleidingen, bevindingen en maatregelen. Afhankelijk van de uitkomst van de analyse, wordt gekeken wanneer deze wordt vermeld in de kamerbrief."*
- **8 december: stand van zakenbrief (Kamerstuk 25295-771)**
 - o *De Kamer wordt geïnformeerd over regie op de testketen: "Om blijvend regie te kunnen voeren over de gehele testketen kijkt de Regiegroep Digitale Ondersteuning Testen, Traceren (DOTT) naar de volledige en actuele dataset van het aantal positieve en negatieve testresultaten. De benodigde digitale ondersteuning zal op elkaar afgestemd dienen te worden. VWS, GGD en RIVM werken aan de risicoanalyse voor de gegevensuitwisseling van de coronatestketen. De rapportage hiervan wordt half december verwacht."*
 - o *Over de verwerking van persoonsgegevens in de testketen: "Laboratoria gebruiken alleen persoonsgegevens die gepseudonimiseerd zijn en dus niet direct herleidbaar zijn tot een persoon. De testuitslagen worden door laboratoria aan de GGD gemeld via **CoronIT**. Hier wordt de uitslag van de test weer gekoppeld aan de persoon.*
 - o *Over de **vaccinatie registratie**: "Daarbij worden de privacy by design principes als uitgangspunt genomen"*
- **8 december: verslag Regiegroep DOTT**
 - o *In het kader van de "Werkgroep Testen vanuit Burgerperspectief" wordt geconstateerd dat "Er moet ook worden gekeken naar de stabiliteit van het*

systeem [CoronIT], een extra schakel in de keten kan zwaktes veroorzaken [zegt GGD]. Daarom oog houden voor duurzame inrichtingen van de keten en keteninformatisering [reactie VWS]."

- Besloten wordt dat GGD en RIVM worden aangehaakt bij de koppeling met CoronIT.
- **10 december: notulen LCT**
 - "De opdrachtomschrijving [voor regiegroep DOTT] is bijgesteld na de eerste bijeenkomst. De opdracht van de regiegroep gaat specifiek over de digitale testketen en vervult daarmee een witte vlek. Vrijdag 11 december 2020 wordt de risicoanalyse opgeleverd. Deze analyse beschrijft een aantal kwetsbaarheden. De acties ten gevolge van deze kwetsbaarheden zullen in de een aparte werkgroep onder de regiegroep worden opgepakt. Deze risicoanalyse zal samen met de IT-audit van KPMG (18 december) per brief aan de minister worden aangeboden."
- **14 december: PO VWS – GGD GHOR**
 - De uitkomsten van de risicoanalyse worden besproken:
 - "Goede duiding risicoanalyse in kamerbrief was het plan. Vanwege andere planning waarschijnlijk deze week een aparte brief. Niet koersen op een apart debat. Goed afstemmen over de inhoud."
- **15 december: verslag Regiegroep DOTT**
 - Het eerste beeld van de follow-up risicoanalyse wordt besproken:
"Afgelopen week zijn de eerste uitkomsten van de risicoanalyse gedeeld. Alle partijen zijn hierbij betrokken en de definitieve versie wordt deze week verwacht. Het rapport heeft een departementaal vertrouwelijke classificatie gekregen i.v.m. cybersecurity en bepaalde kwetsbaarheden. De inhoud van de analyse wordt gedeeld met de kamer via een brief."
"Voor het vervolg van de risicoanalyse wordt een werkgroep opgericht [...] De groep wordt nog samengesteld uit leden van deze regiegroep i.c.m. NCSC voor de onderwerpen rondom cybersecurity."
"Er zijn bepaalde maatregelen die direct uitgevoerd kunnen worden, andere zaken hebben meer en diepgaandere analyse nodig."
 - In de vergadering wordt besloten dat "er wordt gewerkt aan de concept opdrachtformulering voor de werkgroep" en dat GGD en RIVM aansluiten bij deze werkgroep.
- **15 december: Notulen Stuurgroep GGD Contact**
 - In de stuurgroep wordt de wens uitgesproken "in januari wat langer stil te willen staan bij het onderwerp communicatie in de stuurgroep met het oog op meer informatieverstrekking naar de kamer. Op dit moment lijkt die behoefte beperkt"
 - De verwachting wordt uitgesproken dat "uitgebreide nieuwe informatieverstrekking over de vakantie getild wordt." Dit wordt al wel voorbereid: "Hierbij ook letten op het mogelijk opvragen van documenten als de DPIA."
 - VWS geeft aan dat "de GGD'en op moeten letten dat zij op tijd de DPIA vaststellen in een MT of vergelijkbaar gremium om later duidelijk te maken dat er sprake is van een formele vaststelling".
- **16 december: Verslag Bestuurlijk Overleg MVWS – DPG'en**
 - In het kader van "Traceren/BCO" wordt gezegd: "Er wordt opgeschaald volgens de roadmap. Daarnaast wordt er een efficiëntieslag gedaan, waaronder de GGD Contact app."
- **17 december: notulen LCT**
 - Na overleg is de opdrachtformulering voor de regiegroep DOTT aangepast, er is een passage toegevoegd door de GGD.
 - Over de risicoanalyse wordt het volgende gezegd:
"KPMG rapport rond deze tijd. Risicoanalyse wordt vandaag definitief opgeleverd. Risicoanalyse toont serieuze kwetsbaarheden. Moeten we gezamenlijk wat mee. Ook met het NCSC. Er wordt een werkgroep follow-up risicoanalyse ingesteld. Wordt nagedacht over een opdrachtformulering. Kan niet allemaal tegelijkertijd, dus moet een prioritering komen.
Brief die recht doet aan de kwetsbaarheid en recht doet aan eerder gedane inspanningen. Brief voor de Kerst naar de Kamer. Werkprogramma verbeteringen past wel bij de LCT."
- **22 december: verslag Regiegroep DOTT**

- Follow-up risicoanalyse wordt besproken: *"In de eerste week [van januari] wordt de samenstelling [van de werkgroep] afgerond, de tweede week de kick-off."* De GGD sluit zich aan bij dit tijdsplan.
- Om al een snelle slag te kunnen slaan, is een procesvoorstel gemaakt voor escalatie bij bijvoorbeeld storingen. Dit *"keten incidenten managementproces is in gang gezet → kan niet wachten tot half januari om daar stappen in te zetten"*.
- Ook staat in het verslag: *"De werkgroep follow-up risicoanalyse zal fungeren als landingspunt voor (on)gevraagde adviezen over het IT-landschap."*
- **24 december Aanvullende opdracht voorzitter LCT** In deze brief wordt de opdracht verlengd en worden (nieuwe) speerpunten benoemd; een van deze speerpunten is:
 - *"De start en gedeeltelijke uitvoering van een verbeterprogramma DOTT met urgente kortlopende acties t.b.v. veiligheid, datastabiliteit en opschaalbaarheid."*
 - En: *"Afstemming en bewaken in de LCT van de (werk)processen van testen en vaccineren op de GGD-teststraten, in de ICT, etc."*
- **24 december: Kamerbrief met informatie over uitgevoerde risicoanalyse IT-landschap testen en traceren (Kamerstuk 25295-843)**
 - *"De afgelopen tijd is hard gewerkt in samenwerking met alle ketenpartijen om de test- en traceerketen verder te ontwikkelen. Een goede IT-ondersteuning is daarbij een belangrijke randvoorwaarde. Bestaande systemen worden veel grootschaliger ingezet dan voor de crisis en nieuwe systemen worden door enorme inspanningen van verschillende ketenpartners opgezet en ontwikkeld te midden van de crisis. Bij de oploop van de besmettingscijfers zijn enkele keren problemen ontstaan bij het tijdig leveren van data over bijvoorbeeld het aantal positieve testen. Bovendien heb ik de behoefte aan een stabiele informatiestroom om verantwoording af te leggen aan uw Kamer. Daarom is in opdracht van VWS, GGD GHOR Nederland en het RIVM een risicoanalyse uitgevoerd op de IT-systemen en gegevensuitwisseling in de test- en traceerketen 'COVID-19'. Dit om te beoordelen of en waar een versteviging, uitbouw en – waar nodig – herontwerp van de onderliggende ICT-infrastructuur verstandig is. Met deze brief informeer ik uw Kamer over de risicoanalyse van de digitale testketen.*
 - *"De gegevensuitwisseling is te karakteriseren als een estafette: op verschillende momenten in de tijd worden door individuele ketenpartners gegevens aan elkaar overgedragen. Dit betreft meerdere soorten gegevens, zoals persoonsgegevens, testuitslagen, logistieke en stuurgegevens, alsmede data voor onderzoek en rapportage. Over de manier waarop informatie wordt uitgewisseld zijn tussen de ketenpartners afspraken gemaakt. De risicoanalyse legt enkele kwetsbaarheden bloot, onder meer op het gebied van informatiebeveiliging, IT-continuïteit, datakwaliteit en toekomstbestendigheid. In de kern komt het erop neer dat twee van de drie gebruikte IT-systemen in het verleden zijn gebouwd voor verschillende doeleinden, waardoor systemen onvoldoende op elkaar aansluiten. Hierdoor is het IT-landschap niet optimaal geschikt voor gebruik tijdens een pandemiesituatie. Dit veroorzaakte de afgelopen maanden verschillende storingen. Naar aanleiding van die storingen zijn er reeds verbeteringen doorgevoerd en hebben de specialisten van de ketenpartijen elkaar opgezocht. Aanvullend bestaat de behoefte aan keten brede regie. De risicoanalyse is op 11 december jl. in concept opgeleverd en blijft, mede na overleg met het NCSC, vanwege veiligheidsredenen vertrouwelijk."*
 - *"Ik neem naar aanleiding van de risicoanalyse samen met de ketenpartners de volgende maatregelen om daarmee de risico's te beheersen:*
 - *Om het risico op datalekken te minimaliseren wordt een beter passend autorisatiebeheer ingericht. Hierdoor wordt het voor onbevoegde en/of niet-geautoriseerde gebruikers onmogelijk gemaakt om toegang te krijgen tot bepaalde gegevens;*
 - *We zetten hoogwaardige cyber security expertise in om de beveiliging van het huidige systeemlandschap te verbeteren en kwetsbaarheden verder uit te sluiten (met name op het gebied van informatiebeveiliging en bescherming van persoonsgegevens).*
 - *Ik zal de regiegroep DOTT opdracht geven om samen met de ketenpartners op korte termijn het door de Voorzitter Regiegroep reeds ingerichte laagdrempelig incidentproces te formaliseren, zodat we eerder in gezamenlijkheid op de hoogte zijn van incidenten en andere verstoringen, en daar beter en sneller op kunnen reageren. Hierdoor zal*

ik ook tijdig richting publiek en uw Kamer kunnen communiceren over eventuele toekomstige ongeregelheden in de keten. In een later stadium kan dit proces verder uitgewerkt en geprofessionaliseerd worden.

- *Gezien de te verwachten toename van het aantal uitgevoerde testen, zal ik de regiegroep DOTT vragen samen met de ketenpartners te werken aan het verbeteren van schaalbaarheid, performance en stabiliteit in de keten. Ook de eerdergenoemde fundamentele herijking dient daarbij te worden betrokken."*

Januari 2021

- 5 januari: verslag Regiegroep DOTT

- Stand van zaken werkgroep follow-up risicoanalyse wordt besproken. Duidelijk wordt dat de werkgroep nog in de opstartfase zit. Suggestie van VWS "om niet te wachten tot de groep compleet is, maar meteen te beginnen."
- Status incidentmanagement proces wordt besproken: "De eerste notitie is al rondgegaan. Aanleiding: bepaalde incidenten kwamen niet naar boven in de lijn in het verleden. Er moet een acute oplossing komen, zodat incidenten beter en eerder bekend zijn."
- De GGD geeft aan dat er bij hun ook behoefte bestaat dit proces strak neer te zetten: "Binnen de GGD zijn we op zoek naar de governance van escalatie als er een incident is, we zijn er mee bezig dit vast te leggen zodat partijen weten wanneer ze wel/niet worden betrokken. Governance vraag: wie bemoeit zich er allemaal mee? Hoe zou het hele proces gestroomlijnd kunnen worden op dat terrein? Bijv. Wanneer wordt iets ingevoerd in CoronIT?" Afgesproken wordt dat GGD en RIVM meelezen op het incidentmanagementproces.
- GGD licht de IT Audit, uitgevoerd door KPMG, toe: "[Is] grotendeels klaar. Conceptrapportage is beschikbaar. Volgende week woensdag staat de eindbespreking met KPMG, directie GHOR en programmadirectie corona gepland. De DPG raad dient ook nog te worden aangehaakt. Erna komt een terugkoppeling naar de Werkgroep follow-up risicoanalyse en vervolgens ook de Regiegroep DOTT."

- 7 januari: Notulen LCT

De regiegroep DOTT komt ter sprake. Men is "nieuwsgierig naar een tijdlijn". Verder staat er: "Volgende week meeting werkgroep follow-up. Opdrachtformulering gezamenlijk opstellen. Richting kamer aangeven dat we in control zijn. Z.s.m. een planning presenteren in overleg met de ketenpartners."

- 8 januari: Verslag Stuurgroep GGD Contact

- "We wachten met verdere opschaling naar meer BCO'ers totdat het aantal geïnfecteerden lager is en totdat er een oplossing is voor de informatieuitwisseling tussen HPZone en Portaal."

- 12 januari: Verslag Regiegroep DOTT

- Stand van zaken werkgroep follow-up risicoanalyse: "WG zal zich specifiek richten op de korte termijn acties, maar we moeten ook het lange termijn perspectief in beeld houden. Het doel is een duurzame, volwassen keten. Daar zijn zaken voor nodig. Dit moeten we niet uit het oog verliezen in de waan van de dag en wanneer we bezig zijn met korte termijn acties."
- Incidentmanagement proces: "Doel is het signaleren en managen van incidenten op het hoogste niveau." Vraag over eigenaarschap wordt besproken: "Wil/kan vanuit VWS het eigenaarschap gepakt worden? Ligt het eigenaarschap daar waar het incident plaatsvindt? Na escalatie tot het hoogste niveau, ligt dan het eigenaarschap bij VWS of bij het drieman/vrouw verband? Wordt volgende DOTT besproken ter beslissing."

- 12 januari: stand van zakenbrief (Kamerstuk 25295-874)

- De Kamer wordt geïnformeerd over het vaccinatie informatie- en monitoringssysteem CIMS: "Ik kan inmiddels melden dat het COVID-19 vaccinatie informatie- en monitoringssysteem (CIMS) donderdag 7 januari live is gegaan."
- "Ook van de vaccinaties die plaatsvinden bij de GGD-vaccinatie locaties worden de data geregistreerd, via GGD-registratiesysteem CoronIT. Van de GGD'en heb ik vernomen dat het systeem stabiel werkt, zowel voor aanmeldingen en afspraken als voor registratie van gegevens."

- "tot en met 11 januari geeft 96% van de gevaccineerden in ziekenhuizen en 98% van de gevaccineerden in de GGD-vaccinatielocaties toestemming dat hun vaccinatiegegevens (niet-anoniem) worden doorgeleverd."
- Een follow-up op de risicoanalyse van het IT-landschap wordt aangekondigd: "IT-landschap: In de brief van 24 december jl. heb ik uw Kamer geïnformeerd over de uitgevoerde risicoanalyse van het IT-landschap testen en traceren. Hierin werden enkele maatregelen beschreven om de meest acute risico's te mitigeren. Deze week zal de kick-off plaatsvinden van de werkgroep die de follow-up van deze risicoanalyse gaat uitvoeren. In deze werkgroep zijn alle ketenpartners vertegenwoordigd. Het streven is om in februari 2021 nog een eerste schets gereed te hebben van tijdlijnen t.a.v. het verbeterplan op korte termijn."
- Ook wordt de Kamer ingelicht over de vorderingen met betrekking tot GGD Contact:
- "In mijn brief dd. 17 november heb ik u ook geïnformeerd over de ontwikkeling van GGD Contact. Deze digitale oplossing ondersteunt de GGD bij het uitvoeren van bron- en contactonderzoek door het verzamelen en registreren van gegevens te versnellen en vereenvoudigen.
- Samen met de GGD is gekozen voor een gefaseerde aanpak waarin GGD Contact stap voor stap zal worden ingevoerd, te beginnen met een praktijktest. De eerste praktijktesten zijn reeds gestart in Rotterdam-Rijnmond en West-Brabant. Dat houdt in dat GGD-medewerkers in deze regio's bij het opstarten van het bron- en contactonderzoek de besmette persoon zullen vragen om de GGD Contact-app te gebruiken om de correcte contactgegevens van hun nauwe contacten aan te leveren. Hiermee wordt de kans op fouten in gegevensoverdracht kleiner en kan het vervolgproces sneller in gang worden gezet.
- De praktijktest biedt de mogelijkheid om eventuele kinderziekten in de digitale oplossing te signaleren en op te lossen. Daarnaast geeft het de ruimte om het werken met GGD Contact te verenigen met de bestaande werkprocessen en medewerkers te trainen in het gebruik."
- **19 januari: Verslag Regiegroep DOTT**
 - Werkgroep 'Follow-up Risicoanalyse' deelt verslag van de kick-off:
 - "Positief, goeie kick-off. Komende donderdag 21/01 vervolgmeeting. Drie denklijnen:
 - Korte termijn
 - (Middel)lange termijn
 - Innovatie

Donderdag wordt verdeling in groepen geregeld. De Regiegroep wordt op de hoogte gehouden over behoeftes wat betreft bemensing. Voor de lange termijn worden indien nodig professionals aangehaakt op bepaalde onderwerpen. Verzoek vanuit GGD om aandacht te houden voor de impact op lokaal niveau, voorstel om waar relevant impact analyses uit te voeren in de werkgroep."
- **20 januari: Kamerbrief 96e OMT advies deel 2 en kabinetsreactie (Kamerstuk 25295-912)**

De Kamer wordt geïnformeerd over de eventuele quarantaineplicht en dat ook daarvoor de registratie van persoonsgegevens nodig zal zijn: "Om de quarantaineplicht te kunnen handhaven worden de positieve testuitslagen, waarover de GGD beschikt, tijdelijk geregistreerd in een centraal register."
- **Vrijdag 22 januari: Bestuurlijk Overleg MVWS – DPG'en**
 - In het kader van "Traceren" wordt besproken:
 - "De GGD Contact app zal naar verwachting een efficiëncy slag hebben van 25% - 50% in Q1.

De GGD geeft aan dat de GGD Contact app veelbelovend is, maar dat er meer aandacht lijkt te zijn voor de Coronatesten app, onder andere omdat hierbij een datum (1 februari) is genoemd. De GGD vraagt zich af of er ook voor de GGD Contact app een datum kan worden genoemd, zodat er meer ambtelijke power komt.

De minister geeft aan dat hij er voorstander van is om [...] meer prioriteit te geven aan de GGD Contact app."
- **25 januari: RTL4 bericht over datalek GGD door journalist Daniel Verlaan.**
- **26 januari: Mondelinge vragen van het lid Hijink (SP)** aan de Minister van Volksgezondheid, Welzijn en Sport over de handel in privégegevens van miljoenen

Nederlanders uit coronasystemen van de GGD (Rtlnieuws.nl, 25 januari 2021)
(ingezonden 26 januari 2021).

- Minister **De Jonge**: [...] "Sinds de start van de pandemie controleert de GGD uiteraard continu het gebruik van de systemen. In december hebben we samen met de GGD een risicoanalyse laten uitvoeren en zijn er maatregelen getroffen om de beveiliging te verhogen. Zo voldoet het systeem inmiddels aan de laatste norm voor informatiebeveiliging in de zorg, de NEN 7510."
[...]
- "De **voorzitter**:
Als dat strafrechtelijk onderzoek is afgerond, wordt de Kamer daar dan ook over geïnformeerd?
Minister **De Jonge**:
Uiteraard.
De **voorzitter**:
Want ik voel dat er heel veel vragen zijn blijven hangen en onbeantwoord zijn gebleven. Ik begrijp dat dat niet meteen kan, maar misschien kan dat wel binnen een bepaalde termijn.
Minister **De Jonge**:
Dat is altijd aan het Openbaar Ministerie, dus die termijn ken ik niet. Maar ik zet uiteraard wel met de GGD de stappen die nodig zijn om de informatiebeveiliging verder te verbeteren. Ik denk dat het goed is om u daarover in ieder geval te informeren. Dat zal ik binnen een maand doen."

- **26 januari: Verslag Regiegroep DOTT**

- "Er zijn foto's en filmpjes van dossiers gemaakt uit CoronIT. Daarnaast is bekend gemaakt door een journalist dat hij weet dat er datasets gedownload uit HPZone Lite en online te koop aangeboden zijn. Tot heden is hiervoor overigens geen bewijs.

Eerder genomen maatregelen:

- Voldoen aan informatiebeveiligingsnormen
- VOG voor werknemers
- Geheimhoudingsverklaringen werknemers
- Beveiligen van verkeersstromen van en naar applicaties

Maatregelen CoronIT:

- Alle applicaties worden nagegaan en de downloadfunctie wordt waar mogelijk beperkt, ook als dit functioneel nut heeft.
- Toepassen van dataminimalisatie.
- Niet toegestaan om cameratoezicht en blacklisting toe te passen ter voorkoming van het maken van foto's/filmpjes van de dossiers
- Verdere beperking en specificering van zoekresultaten en downloads door medewerkers.

Maatregelen HPZone:

- Functionaliteit om datasets te downloaden verwijderd
- Forensisch onderzoek loopt naar sporen van logging & onderzoek loopt naar waar datasets te koop zijn.
- Monitoring software (security incident and even monitoring (SIEM)) versneld uitgerold.

Veel sympathie vanuit de andere ketenpartners, die ook aangeven bereid te helpen waar nodig/gewenst.

Alle effort op het zsm implementeren van GGD Contact en het minimaliseren van het gebruik van HPZone."

- Ook wordt GGD Contact toegelicht:
- "GGD Contact is ontwikkeld ter bevordering van het digitaal contact tussen de index en BCO medewerker. Aanleiding is kwalitatief verbeteren BCO en efficiënter maken ervan, verslaglegging neemt nu veel tijd in beslag."
- "Doelen: verminderen tijdsbesteding administratie BCO, sneller handelingsperspectief, verhoogde kwaliteit contactgegevens, groter bereik aantal contacten."
- "Gebruiksvriendelijkheid en harmonisatie van werkprocessen lokale GGD-en is leidraad. App [...] voldoet aan alle beveiligingseisen."
- "Functionaliteiten: contacten toevoegen door index, aanvullen contacten na BCO-gesprek. Backlog BCO-portaal: contexten toevoegen, ook gebruiken als index de app niet heeft, opnemen van volledige BCO vragenlijst, automatische case samenvatting, automatisch ingevulde Osiris vragenlijst, functionaliteit voor

monitoren van contacten inclusief aanduiding belmomenten; datavelden voor en automatische rapportages tav contactmonitoring, datavelden voor en automatische rapportage clusters/outbreaks, en andere datavelden en functionaliteiten zoals HPZone deze nu bevat en zoals deze gebruikt worden in regionale en landelijke surveillance tbv het zicht houden op en het inzicht hebben in de verspreiding van het virus (een van de drie pijlers van het kabinet)."

- "Afgelopen maanden discussie gevoerd over koppeling HPZone, na incident kunnen we niet anders dan dat systeem omzeilen. Maar alsnog belangrijke elementen uit HPZone die moeten worden gewaarborgd → clusteranalyses en koppeling naar Osiris etc." [...] "Consequenties zijn fors voor clusteranalyses en melden van contacten, Osiris koppeling. Vraag is consequenties van omzeilen HPZone." [...] "Oproep vanuit DOTT richting GGD om niet te aarzelen om hulp in te roepen waar nodig."
- "GGD datalek roept bij mij zorgen op voor ICT spoor 2 (testen zonder symptomen), goed na gaan wat we allemaal gaan vastleggen van mensen, met name betreffende de negatieve testresultaten, wat de overgrote meerderheid van de meldingen zal zijn. [...] Graag verkennen wat de mogelijkheid is om geen gegevens op te slaan van negatief geteste mensen."
- **28 januari: Notulen LCT**
 - GGD GHOR licht toe: "extreem vervelend incident met datadiefstal. Onderscheid maken tussen coronIT en HPZone. CoronIT medewerkers gezocht en data gestolen. Twee aanhoudingen. Wat verbeterd kan worden in coronIT dat je op achternaam icm met geslacht kunt zoeken. We zetten dat nu meer dicht door in combinatie met NAW te zoeken. Verder CoronIT niet enorme zwakheden. In HPZone zat een downloadknop voor alle users. Daar is misbruik van gemaakt. De knop is inmiddels uitgezet. Bezig op dat gat verder te dichten, maar dat is niet heel makkelijk."
 - De voorzitter constateert dat er tijd verloren is gegaan bij het inrichten van de regiegroep DOTT: "Tijdsverlies is opgetreden in het beraden op de inrichting van DOTT. Is achteraf kijken. Cruciaal om nu te weten wat we op korte, middellange en lange termijn moeten oplossen. Verbeterplan wordt door DOTT binnenkort opgeleverd. Graag in volgende LCT vergadering vanwege de urgentie."
- **Op 27 januari publiceert de Autoriteit Persoonsgegevens (AP)** een persbericht: "De Autoriteit Persoonsgegevens (AP) heeft direct opheldering geëist bij de GGD."
- **28 januari: Convenant Versterking Testketen Corona** wordt gepubliceerd in de Staatscourant van het Koninkrijk der Nederlanden.