Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

27 529 **Informatie- en Communicatietechnologie (ICT) in de Zorg**

32 761 **Verwerking en bescherming persoonsgegevens**

Nr. 234

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 4 februari 2021

De vaste commissie voor Volksgezondheid, Welzijn en Sport heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Volksgezondheid, Welzijn en Sport over de brief van 2 februari 2021 over «GGD wist al maanden van privacyproblemen».

De vragen en opmerkingen zijn op 29 januari 2021 aan de Minister van Volksgezondheid, Welzijn en Sport voorgelegd. Bij brief van 2 februari 2021 zijn de vragen beantwoord.

De voorzitter van de commissie,
Lodders

Adjunct-griffier van de commissie,
Heller

kst-27529-234
ISSN 0921 - 7371
's-Gravenhage 2021

Vragen en opmerkingen vanuit de fracties en reactie van de bewindspersoon

Inleiding

Vooraf wil ik u melden dat ik mij voor de antwoorden op deze vragen baseer op de mij nu beschikbare informatie, die ik in korte tijd heb moeten verzamelen. Daarbij is een groot deel van de antwoorden gebaseerd op informatie die is aangeleverd door de GGD GHOR. Gegeven het korte tijdsbestek kan ik niet uitsluiten dat er aanvullende informatie beschikbaar komt.

Vragen en opmerkingen van de VVD-fractie

De leden van de VVD-fractie hebben met zorgen kennisgenomen van het bericht over het datalek bij de coronasystemen van de Gemeentelijke Gezondheidsdienst (GGD). Genoemde leden vinden dat te allen tijde zorgvuldig en vertrouwelijk moet worden omgegaan met grote hoeveelheden persoonsgegevens. Deze leden vinden het daarom zeer schokkend dat medewerkers van de GGD misbruik hebben gemaakt van hun positie en persoonsgegevens wederrechtelijk hebben verkregen, met als doel deze aan te bieden aan derden. Voor deze leden zijn er drie hoofdvragen die zij graag beantwoord zien:

1. Hoe groot is de omvang van het datalek en hoe heeft dit kunnen gebeuren?
De GGD heeft mij gemeld dat de omvang van de datadiefstal en de precieze gang van zaken nu nog niet bekend zijn. Dit maakt onderdeel uit van het politieonderzoek.

2. Wat heeft de Minister gedaan om het lek te stoppen?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd (Kamerstuk 27 529, nr. 235).

3. Hoe informeert de Minister de slachtoffers?
De GGD heeft mij gemeld dat op dit moment onduidelijk is wat de omvang is van het aantal data dat gestolen is. Dat is onderdeel van het politieonderzoek.
De GGD heeft mij gemeld dat wanneer bekend is van welke personen informatie gestolen is, de GGD hen zal informeren. Burgers moeten te allen tijde kunnen vertrouwen dat medische gegevens veilig worden gedeeld en bewaard, juist vanwege het privacygevoelige karakter van deze gegevens. Incidenten als deze zijn zeer ernstig voor de mogelijke slachtoffers, het vertrouwen heeft schade opgelopen en dat betreur ik.

Aanvullend hierop hebben de leden van de VVD-fractie meerdere vervolgvragen.

4. De leden van de VVD-fractie vragen de Minister welke maatregelen hij had getroffen om datalekken te voorkomen in de systemen van de GGD?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

5. Welke aanvullende maatregelen heeft de Minister genomen nadat hij in december aan de Kamer schreef dat er een risico was op datalekken?
Onder de Regiegroep DOTT is de werkgroep follow-up risicoanalyse opgericht, met als opdracht de digitale ondersteuning in de test- en traceerketen te verbeteren en verduurzamen. Daarnaast is er door de GGD een aparte IT-audit uitbesteed, waarvan de resultaten op 30 januari jl. met mij zijn gedeeld.

6. Klopt het dat de GGD (medische) persoonsgegevens verwerkte, terwijl de organisatie nog niet aan de Nederlandse Norm (NEN)-norm voldeed?
De GGD heeft mij gemeld dat binnen de 25 GGD'en verschillende kwaliteitssystemen worden gehanteerd (onder andere HKZ). GGD GHOR Nederland bereidt zich voor op certificering volgens NEN 7510.

Tijdens het vragenuur op 26 januari jl. (Handelingen II 2020/21, nr. 48, mondelinge vragen van het lid Hijink over de handel in privégegevens van miljoenen Nederlanders uit coronasystemen van de GGD) stelde de Minister dat van de GGD verwacht mag worden dat sollicitanten aan de voorkant goed worden gescreend, voordat zij worden aangenomen dus.
7. Kan de Minister aangeven hoe deze screening eruitziet en/of dit proces identiek is voor alle medewerkers van de GGD én medewerkers van externe partijen?
De GGD heeft mij gemeld dat mensen een Verklaring Omtrent het Gedrag (VOG) moeten aanleveren en een geheimhoudingsverklaring ondertekenen. Dit is van toepassing op medewerkers van de GGD'en en van externe partijen.

8. Klopt het dat medewerkers die niet in het bezit zijn van een verklaring omtrent gedrag (VOG) toegang hebben gehad tot (medische) persoonsgegevens?
De GGD heeft mij gemeld dat medewerkers van GGD'en en externe partijen een Verklaring Omtrent het Gedrag (VOG) moeten aanleveren. Gegeven de snelheid waarmee de GGD'en en GGD GHOR Nederland hun personele capaciteit moesten uitbreiden, kunnen zich situaties hebben voorgedaan waarin medewerkers wel toegang hadden tot systemen, maar nog geen VOG hadden overlegd.

9. Klopt het dat medewerkers die in het bezit zijn van een strafblad toegang hebben gehad tot (medische) persoonsgegevens?
De GGD heeft mij gemeld dat een VOG wordt verstrekt op basis van een toetsing op het profiel dat voor de betreffende functie is vastgesteld. Het kan zijn dat medewerker veroordeeld is voor strafbare feiten die niet relevant zijn voor de functie waarvoor de VOG is aangevraagd.

10. Hoe kon het gebeuren dat medewerkers zonder VOG (medische) persoonsgegevens konden inzien?
Voor het antwoord op deze vraag verwijs ik u naar het antwoord op vraag 8.

11. Aan welke voorwaarden moeten medewerkers van de GGD voldoen om toegang te krijgen tot gevoelige informatie?
Voor het antwoord op deze vraag verwijs ik u naar het antwoord op vraag 7.

12. Hoeveel medewerkers voldoen aan deze voorwaarden en wordt gecontroleerd of medewerkers aan deze voorwaarden voldoen?
De GGD heeft mij gemeld dat in totaal bij de 25 regionale GGD'en, GGD GHOR Nederland en gecontracteerde partijen ruim 26.000 mensen betrokken zijn bij testen en vaccineren en ruim 20.000 bij bron- en contactonderzoek. Het is denkbaar dat daar ook medewerkers tussen zitten die niet aan deze voorwaarden voldoen. Een exact aantal is niet te geven gezien de aantallen en de verschillende arbeidsrelaties. Elk van deze werkgevers hanteert zijn eigen controle-systematiek.

13. Tot op welk niveau in het systeem hebben medewerkers toegang tot gevoelige data?
De GGD heeft mij gemeld dat de medewerkers in HPZone toegang hadden tot de exportfunctie, dus ook tot gevoelige data. Deze functie is inmiddels

slechts toegankelijk voor een beperkte groep medewerkers. In CoronIT konden medewerkers ook meerdere dossiers inzien, maar niet in grote aantallen tegelijk.

14. Kan de Minister voorts aangeven hoe het autorisatieproces om toegang te krijgen tot gevoelige informatie eruitziet, wie verantwoordelijk is voor het beheer van dit autorisatieproces en wie de eigenaar is van het registratiesysteem?
De GGD heeft mij gemeld dat HPZone is aangesloten op de centrale autorisatievoorziening. De autorisaties zelf worden toegekend door de GGD'en en ingericht in hun eigen identity provider, die gekoppeld is aan de centrale voorziening. Toekenning van autorisaties gebeurt onder verantwoordelijkheid van de regionale GGD'en. Binnen CoronIT worden lokaal autorisaties toegekend.

15. Op welke manier wordt geregistreerd welk persoon welk type gevoelige informatie heeft ingezien? Kan daarbij ook achterhaald worden welke functionaliteiten deze persoon heeft gebruikt tijdens het inzien van deze gevoelige informatie?
De GGD heeft mij gemeld dat in HPZone en CoronIT wordt gelogd welke toegang een gebruiker tot de applicatie heeft gehad. Voor een groot aantal handelingen kan achterhaald worden welke persoon deze heeft gebruikt.

16. Waarom hadden niet enkel de medewerkers voor wie dit noodzakelijk was, toegang tot gegevens in persoonsdossiers?
De GGD heeft mij gemeld dat het doel van de GGD'en is om het COVID-19-virus zo goed mogelijk bestrijden. Daarbij zijn zeer veel medewerkers betrokken. Elke callcenter medewerker die telefoontjes aanneemt (inbound) moet bijvoorbeeld afspraken kunnen maken. En iedere callcenter medewerker die mensen belt (outbound) moet uitslagen door kunnen gegeven als deze binnen zijn. Bij het bron- en contactonderzoek moeten medewerkers uit verschillende regio's en de landelijke schil toegang tot dossiers hebben om elkaar te kunnen ondersteunen bij het snel doorgeven van testuitslagen en op piekmomenten in de aantallen besmettingen.

17. De leden van de VVD-fractie vragen de Minister voorts of het klopt dat de exporteer-functionaliteit inmiddels verwijderd is? Kan de Minister aangeven met welk doel deze functionaliteit ingebouwd is?
De GGD heeft mij gemeld dat CoronIT geen exportfunctionaliteit heeft. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Het uitzetten van de printfunctionaliteit levert geen problemen op voor het operationeel proces. HPZone heeft zowel een export- als een printfunctionaliteit.De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziektenbestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers. Met de printfunctionaliteit kan de medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen. De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat

alsnog gebeurd. Als gevolg van deze maatregelen kunnen de medewerkers nu minder efficiënt werken.

18. Klopt het dat de GGD pas eind maart systemen heeft die automatisch en continu zullen controleren op misbruik?
De GGD heeft dit bevestigd. Systemen worden aangepast, maar dat kost tijd. Tot de start van automatisch en continu monitoren eind maart, blijven gespecialiseerde interne en externe teams voor de GGD'en de loggings controleren.

19. Hoe garandeert de Minister dat de persoonsgegevens van mensen die zich laten testen of vaccineren voortaan veilig zijn?
De medische gegevens die bij vaccinaties worden vastgelegd zijn afgeschermd voor medewerkers van de GGD die zich bezighouden met testen. Naar aanleiding van het incident dat heeft plaatsgevonden heeft de GGD de zoekfunctie van CoronIT beperkt en worden de loggings gecontroleerd om verdacht gedrag te identificeren, hiermee wordt de beveiliging van persoonsgegevens van mensen die zich hebben laten testen aangescherpt. Er wordt alles op alles gezet om persoonsgegevens beter te beveiligen.

Gelet op het feit dat ook persoonsgegevens bij het vaccinatieproces geregistreerd en gedeeld worden, en hierbij ook verschillende registratiesystemen aan elkaar gekoppeld moeten worden, willen de leden van de VVD-fractie een klemmende oproep doen om te zorgen dat deze persoonsgegevens zo goed mogelijk beschermd worden.

20. Tijdens het coronadebat over vaccinatie op 17 december jl. (Handelingen II 2020/21, nr. 39, debat over berichtgeving dat vaccinatie tegen het coronavirus niet meer in 2020 start), stelde de Minister dat er nog veel discussie was over de condities waarbij gegevens kunnen worden gedeeld. Kan de Minister aangeven welke stappen er sindsdien zijn gezet? Zijn er al condities bekend waarbij gegevens gedeeld kunnen worden en zo ja, welke zijn dit?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

21. De leden van de VVD-fractie vragen of er, naast de twee verdachten die nu zijn opgepakt, nog meer mensen verdacht worden van het misbruiken van de informatie van de GGD?
Het openbaar ministerie heeft vorige week twee verdachten aangehouden en voorgeleid ter zake van datadiefstal bij de GGD. De rechter-commissaris bepaalde dat beide verdachten voorlopig langer blijven vastzitten. Uit nader onderzoek moet blijken wie welke rol heeft gehad. Meer aanhoudingen worden niet uitgesloten. Het bericht afkomstig van de GGD dat er inmiddels meer verdachten zouden zijn aangehouden is onjuist en is door de GGD gecorrigeerd. Aangezien het een nog lopend opsporingsonderzoek betreft verzet het opsporingsbelang zich er op dit moment tegen Uw Kamer van meer informatie te voorzien.

22. Welke acties onderneemt de Minister om de handel in de al buitgemaakte (medische) persoonsgegevens te stoppen?
Het openbaar ministerie heeft naar aanleiding van een melding van mogelijke datadiefstal bij de GGD onmiddellijk actie ondernomen door een opsporingsonderzoek te starten en heeft kort na de start van dit onderzoek twee verdachten aangehouden en voorgeleid. Daarbij zijn onder meer telefoons in beslag genomen en wordt berichtenverkeer in kaart gebracht. Het stelen van data en het verhandelen ervan is strafbaar gesteld en het openbaar ministerie treed daar zoals in het onderhavige

geval adequaat tegen op. Of en zo ja in welke mate de data zijn verhandeld is nog in onderzoek.

23. Zijn er signalen van misbruik van de buitgemaakte (medische) persoonsgegevens? Diefstal van persoonsgegevens kan aanleiding geven tot misbruik, bijvoorbeeld voor het plegen van identiteitsfraude. Of en zo ja in welke mate er in het onderhavige geval sprake is (geweest) van misbruik is nog in onderzoek.

Vragen en opmerkingen van de PVV-fractie

De leden van de PVV-fractie hebben met ontzetting kennisgenomen van de grootschalige handel in persoonsgegevens uit de coronasystemen bij de GGD. Het gaat om privacygevoelige informatie van namen en adresgegevens, telefoonnummers, burgerservicenummers (BSN's) en testuitslagen van miljoenen Nederlandse burgers. Genoemde leden stellen vast dat hier sprake is van een ernstig misdrijf en roepen de Minister op onmiddellijk te zorgen voor een veilig coronasysteem. Daarnaast hebben deze leden de volgende kritische vragen en opmerkingen. De leden van de PVV-fractie zijn geschokt dat de illegale handel in coronadata al maanden aan de gang is.

24. Hoe kan het zijn dat dit niet eerder is gesignaleerd? Worden er geen steekproeven afgenomen? Waarom zijn nergens alarmbellen afgegaan?
De GGD heeft mij gemeld dat controles structureel steekproefsgewijs plaats vinden. In de afgelopen periode heeft dat circa 30 keer tot ontslag geleid. Inmiddels wordt automatische en continue monitoring voorbereid. Verder verwijs ik u naar het antwoord op vraag 18.

Genoemde leden vinden een VOG-verklaring en een geheimhoudingsplicht voor GGD-medewerkers volstrekt onvoldoende als blijkt dat hierop niet actief wordt gehandhaafd.
25. Klopt het dat niet alle medewerkers een VOG-verklaring hebben? Zo ja, om hoeveel medewerkers gaat het? Zo ja, hoe gaat de Minister bewerkstelligen dat zij wel een VOG-verklaring gaan overleggen?
De GGD heeft mij gemeld dat in totaal bij de 25 regionale GGD'en, GGD GHOR Nederland en gecontracteerde partijen ruim 26.000 mensen betrokken bij testen en vaccineren en ruim 20.000 bij bron- en contactonderzoek zijn. Het is denkbaar dat daar ook medewerkers tussen zitten die niet aan deze voorwaarden voldoen. Een exact aantal is nu niet te geven. GGD GHOR Nederland zal de regionale GGD'en en gecontracteerde partijen opnieuw vragen daarover informatie te geven.

26. Wat gaat de Minister doen om te bewerkstelligen dat medewerkers die geen VOG-verklaring kunnen overleggen niet voorde GGD kunnen werken?
GGD GHOR Nederland en de GGD'en hebben mij gemeld dat zij willen dat elke medewerker een VOG overlegt en een geheimhoudingsverklaring ondertekent. GGD GHOR Nederland zal het belang daarvan nogmaals benadrukken bij de regionale GGD'en en gecontracteerde partijen.

27. Wat de geheimhoudingsplicht waard is, blijkt wel uit de grootschalige handel die nu aan het licht is gekomen. Welke sanctie staat er op het schenden van de geheimhoudingsplicht en hoe vaak is deze sanctie opgelegd?
De GGD meldt mij dat het schenden van de geheimhoudingsplicht kan leiden tot ontslag. Dat is bij de GGD'en en de gecontracteerde partijen in de afgelopen periode circa 30 keer het geval geweest.

28. De leden van de PVV-fractie vinden dat veel te veel informatie wordt verzameld van burgers. Genoemde leden willen weten welke informatie nu precies in de coronasystemen van de GGD staan en waarom het nodig is om voor een simpele coronatest zoveel informatie op te slaan?
De GGD heeft mij gemeld dat volledige persoonsgegevens nodig zijn, zodat zeker is dat een test- of vaccinatie-afspraak met de juiste persoon wordt gemaakt. In CoronIT, het systeem voor testen en vaccineren, staan naam, adres, woonplaats, telefoonnummer/e-mailadres, BSN, geslacht, geboortedatum, test- en/of vaccineerafspraken en testresultaten. Contra-indicaties en COVID-19 klachten. De gegevens zoals geregistreerd in CoronIT zijn opgenomen in de privacyverklaring CoronIT. Het BSN is noodzakelijk voor de controle van de identiteit. BSN is daarnaast belangrijk, zodat in CoronIT automatisch de juiste persoonsgegevens geregistreerd worden in plaats van dat alle persoonsgegevens handmatig ingevoerd moeten worden (met het risico op administratieve fouten). Daarnaast is het BSN gekoppeld aan DigiD, wat het mogelijk maakt om de uitslag online in te zien. Het woonadres is nodig, zodat de GGD'en de uitslag ook per brief kunnen toesturen indien er onverhoopt een verkeerd telefoonnummer is geregistreerd en daardoor iemand de uitslag niet heeft kunnen ontvangen.

29. Kan de Minister duidelijk maken welke gegevens de GGD vastlegt in het kader van het testen en het bron- en contactonderzoek?
De GGD heeft mij gemeld dat in HPZone naam, adres, woonplaats, telefoonnummer, geslacht, geboortedatum en BSN van een persoon staan. Verder wordt in HPZone ook de informatie uit de bron- en contact-onderzoek gesprekken vastgelegd. Dit zijn onder andere: gegevens over COVID-19-gerelateerde klachten/symptomen en huisarts, waar iemand is geweest en met wie hij/zij in contact is geweest. De gegevens zoals geregistreerd in HPZone zijn terug te vinden in de privacyverklaring van bron- en contactonderzoek in het kader van COVID-19.

30. Kan de Minister per dataveld aangeven wat de noodzaak is van het registreren van het dataveld in de onderhavige IT-database? Wil de Minister hierbij met name ingaan op de persoonsgebonden velden, zoals het BSN, de NAW-gegevens et cetera?
De GGD heeft mij gemeld dat in CoronIT naam, adres, woonplaats, telefoonnummer/e-mailadres, BSN, geslacht, geboortedatum, test- en/of vaccineerafspraken en testresultaten staan. Contra-indicaties en COVID-19 klachten. In HPZone staan naam, adres, woonplaats, telefoonnummer, geslacht, geboortedatum en BSN van een persoon. Verder wordt in HPZone ook de informatie uit de bron- en contactonderzoek gesprekken vastgelegd. Dit zijn onder andere: gegevens over COVID-19-gerelateerde klachten/symptomen en huisarts waar iemand is geweest en met wie hij/zij in contact is geweest.

31. Wat wordt in het kader van een coronatest verstaan onder noodzakelijke informatie?
Voor het antwoord verwijs ik u naar het antwoord op vraag 28.

32. Waarom is de Minister van mening dat de GGD adresgegevens nodig heeft wanneer iemand zelf naar een teststraat toekomt?
De GGD neemt de Covid-19 testen af als zorgverlener. De GGD heeft in het kader van testen een behandelovereenkomst met de betrokkene. Die overeenkomst geeft de basis om persoonsgegevens te verwerken. In dit kader heeft de GGD als zorgaanbieder de verplichting het Burgerservice-nummer (BSN) te registreren van betrokkene en ook een medisch dossier bij te houden op grond van de Wet op de Geneeskundige behandelings-overeenkomst (Wgbo), waarin op basis van BSN geregistreerd moet worden. In dit kader is het ook logisch dat NAW gegevens van betrokkene

worden verwerkt om betrokkene te kunnen bereiken. Het gaat niet om een eenmalige handeling waarvoor een tijdelijke code kan worden gebruikt. Het gaat hier om een zorghandeling, waarbij de GGD als zorgverlener optreedt. Overigens, ben ik niet de verwerkingsverantwoordelijke in de zin van de AVG. De GGD is eigenstandig verantwoordelijk in de zin van de AVG en zij bepaalt ook zelf welke gegevens noodzakelijk zijn te verwerken in het kader van haar taken.

33. Waarom is de Minister van mening dat de GGD het BSN-nummer van iemand nodig heeft voor het afnemen van een test? Waarom kan niet worden volstaan met een eenmalige, tijdelijk afgegeven code?
Voor het antwoord verwijs ik u naar het antwoord op vraag 32.

34. Hoe lang worden welke gegevens bewaard?
De GGD heeft mij gemeld dat zij zich houden aan de wettelijke termijnen die hiervoor gelden. Art 29 Wpg geeft een bewaartermijn van ten hoogte 5 jaar voor de meldingsgegevens die de GGD'n op grond van de Wpg ontvangt. Het gaat daar om de gegevens op grond van artikel 24,25 en 30 Wpg. De GGD'en verwijderen de meldingsgegevens als deze niet langer noodzakelijk zijn, met een maximale bewaartermijn van 5 jaar. De GGD'en bewaren de gegevens in ieder geval voor de gehele duur van de pandemie. Er geldt een bewaartermijn van 20 jaar voor het medisch dossier voor de handelingen waar de GGD als zorgverlener optreedt en een behandelingsovereenkomst heeft met betrokkene. Dat is het geval bij testen en vaccineren door de GGD. Daarvoor geldt vanuit de Wgbo dat de hulpverlener een medisch dossier bijhoudt en 20 jaar bewaart.

35. Is bij de bouw van het coronasysteem overleg geweest met deskundigen en privacyexperts over de informatievergaring en de beveiliging daarvan?
De GGD'en hebben mij gemeld dat overleg is geweest met deskundigen van drie verschillende externe partijen en privacy experts voor en tijdens de bouw van CoronIT. Tijdens de bouw zijn risico's geïdentificeerd en maatregelen getroffen om deze risico's te mitigeren.

36. Wordt de verkregen informatie gedeeld met andere partijen, bijvoorbeeld voor statistische doeleinden?
De GGD heeft mij gemeld dat conform de geldende wet- en regelgeving gepseudonimiseerde gegevens worden gedeeld met het RIVM en op korte termijn ook met het CBS ten behoeve van statistische analyses.

37. Wat is de bewaartermijn voor de data die wordt vergaard?
Voor het antwoord verwijs ik u naar het antwoord op vraag 34.

38. Bestaat er een koppeling met het medisch dossier of met andere medische gegevens van de betrokken personen? Zo ja, waarom?
De GGD heeft gemeld dat in CoronIT testuitslagen en vaccinatiegegevens zijn opgenomen. In HPZone staat eventuele medische informatie die uit het bron- en contactonderzoek blijkt. Uit geen van beide systemen bestaan koppelingen met medische gegevens in andere systemen.

39. Voorts vragen de leden van de PVV-fractie de Minister waarom al deze privacygevoelige informatie toegankelijk is voor minstens 26 duizend GGD-medewerkers. Kan de Minister aangeven hoeveel medewerkers daadwerkelijk toegang hebben tot de genoemde GGD-systemen?
De GGD heeft mij gemeld dat de medewerkers toegang hebben tot persoonsgegevens in CoronIT nodig om afspraken te kunnen maken voor testen en vaccineren. Zij hebben ook toegang nodig tot persoonsgegevens in HPZone (Lite) om bron- en contactonderzoek te kunnen uitvoeren. In totaal zijn bij de 25 regionale GGD'en, GGD GHOR Nederland

en gecontracteerde partijen ruim 26.000 mensen betrokken bij testen en vaccineren en ruim 20.000 bij bron- en contactonderzoek.

40. Welke noodzaak c.q. bedrijfsbelang is er dat rechtvaardigt dat al deze medewerkers toegang hebben tot de volledige inhoud van de databases?
De GGD heeft mij gemeld dat in CoronIT medewerkers toegang hebben tot alle dossiers, maar niet tot alle gegevens in die dossiers. Welke gegevens toegankelijk zijn, is afhankelijk van hun rol. De landelijke toegang is noodzakelijk omdat iedereen die in Nederland verblijft kan bellen om een testafspraak maken en vrije keuze heeft voor de locatie waar zij zich willen laten testen. In HPZone hebben medewerkers alleen toegang tot de gegevens uit de regio('s) waarvoor zijn op dat moment werkzaam zijn.

41. Kunnen al deze medewerkers deze data ook exporteren naar een bestand of andere gegevensdragers?
De GGD heeft mij gemeld dat CoronIT geen exportfunctionaliteit heeft. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Het uitzetten van de printfunctionaliteit levert geen problemen op voor het operationeel proces. HPZone heeft zowel een export- als een printfunctionaliteit.De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziektenbestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers. Met de printfunctionaliteit kan de medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen. De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat alsnog gebeurd. Als gevolg van deze maatregelen kunnen de medewerkers nu minder efficiënt werken.

42. Is er interne controle op wie dit soort specifieke handelingen binnen de database heeft uitgevoerd? Wordt een systeem van persoonsgebonden logging van de activiteiten binnen de databases gehanteerd? Hoe vaak wordt hierover intern gerapporteerd naar de directie van de GGD en wanneer gebeurde dit voor het laatst?
De GGD heeft mij gemeld dat een groot aantal typen handelingen wordt vastgelegd waarbij persoonsinformatie wordt verwerkt. Over deze logging wordt niet gerapporteerd aan de directie van de GGD. Indien uit de logging blijkt dat ongeoorloofde handelingen zijn uitgevoerd, wordt dit aan de leidinggevende van de betrokken medewerker gemeld.

43. Wat zijn de interne aanbevelingen geweest en kan de Kamer hier een exemplaar van ontvangen?
De GGD heeft mij gemeld dat risicoanalyses bevatten vertrouwelijke informatie en om veiligheidsredenen niet worden kunnen gedeeld met de Kamer.

44. Klopt het dat het huidige systeem de mogelijkheid biedt te werken met functieprofielen met niveaus van toegankelijkheid, maar dat alle medewerkers gemachtigd zijn en/of waren belangrijke data te exporteren? Zo nee, hoe is de situatie dan wel? Zo ja, hoe kon dit gebeuren?

De GGD heeft mij gemeld dat exportfuncties in HPZone beschikbaar waren voor alle reguliere rollen. Deze functies dateren uit de situatie waarin er zeer kleinschalig binnen kleine teams bij GGD'en werd gewerkt aan de infectieziektenbestrijding. De toegang tot exportfuncties is inmiddels sterk beperkt.

45. Waarom kent het systeem een exportfunctie, waardoor het zo is dat iedere medewerker grootschalig data kan overzetten en versturen?
Voor het antwoord op deze vraag verwijs ik u naar vraag 44.

46. Waarom kan een medewerker uit Groningen bij testuitslagen uit Limburg?
De GGD heeft mij gemeld dat bron- en contactmedewerkers van een GGD soms tijdelijk toegang kunnen krijgen tot gegevens van een andere GGD om te ondersteunen bij hoge druk. Verder is er een landelijke schil van BCO medewerkers. Deze landelijke BCO medewerkers werken vaak voor meerdere GGD-en en hebben dus toegang tot de gegevens van deze GGD-en. De procedures voor het toegang geven en -na afronding van werkzaamheden- ontnemen, voor landelijke BCO medewerkers en GGD medewerkers die ondersteuning hebben geboden bij een andere GGD worden op dit moment kritisch herzien.

47. Waarom moet het tot eind maart duren voordat het systeem automatisch en permanent gemonitord wordt?
De GGD heeft mij gemeld dat systemen worden aangepast. Dat kost tijd. Tot de start van automatisch en continu controleren eind maart, blijven gespecialiseerde interne en externe teams voor de GGD'en de loggings controleren.

48. Betekent dit dat de illegale handel in coronadata gewoon kan doorgaan? Het openbaar ministerie zorgt ervoor dat strafbare feiten worden opgespoord en vervolgd.
Het openbaar ministerie zorgt ervoor dat strafbare feiten worden onderzocht.

49. Zijn er externe IT-deskundigen ingeschakeld die het systeem op dit moment doorlichten op alle mogelijke datalekken?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd (Kamerstuk 27 529, nr. 236).

50. Wanneer is voor het laatst door een externe partij, bijvoorbeeld door een betrokken accountant of een ander gespecialiseerd bedrijf, een IT-systems audit en/of een IT-risk en control framework audit uitgevoerd, om de interne IT-controlerisico's en bedrijfsrisico's in kaart te brengen? Hoe luidde dit oordeel van de accountant c.q. de auditor?

51. Welke aanbevelingen zijn gedaan?
De GGD heeft mij gemeld dat er in december 2020 een IT-assessment heeft plaatsgevonden op het IT landschap van de COVID-19-bestrijding door GGD GHOR Nederland. Dit assessment heeft geleid tot aanbevelingen waaraan GGD GHOR Nederland uitvoering geeft. Verder verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

52. Wat is het tijdspad van de invoering van deze aanbevelingen en hoe staat het op dit moment met de invoering hiervan?
De GGD heeft mij gemeld dat een deel van de aanbevelingen direct gepland is en een deel daarvan al geïmplementeerd. Andere aanbevelingen zijn onderdeel van lopende projecten en worden de komende weken en maanden doorgevoerd.

53. Kan de Kamer een kopie van deze aanbevelingen ontvangen?
De GGD heeft mij gemeld dat risicoanalyses vertrouwelijke informatie bevatten en om veiligheidsredenen niet kunnen worden gedeeld met de Kamer.

54. Als er recent geen IT-audit door een externe partij is uitgevoerd, weet de Minister of de GGD dan voornemens is dit alsnog met spoed te doen?
De GGD heeft mij gemeld dat de GGD GHOR Nederland met regelmaat audits en assessments laat uitvoeren op onderdelen van het ICT landschap en/of bij de introductie van nieuwe componenten.

55. In de berichtgeving wordt gesproken over twee coronasystemen. Hoeveel systemen zijn er in totaal? Wordt via deze systemen allemaal dezelfde informatie verzameld?
De GGD heeft mij gemeld dat CoronIT en HPZone (Lite) de centrale systemen zijn die de GGD'en gebruiken. De systemen hebben elk een eigen doel. HPZone (Lite) wordt gebruikt voor het bron- en contactonderzoek; CoronIT bij het testen en vaccineren.

56. Per wanneer zijn de systemen veilig?
De GGD heeft mij gemeld dat sinds de zomer van 2020 diverse maatregelen getroffen zijn om het toegangsbeheer te verscherpen en om controles uit te voeren op de toegang tot en het gebruik van persoonsgegevens. Gedurende de gehele periode zijn autorisaties verscherpt, waarbij bij CoronIT in eerste instantie aandacht is uitgegaan naar de scheiding van rollen en inrichting van de rollen, vervolgens naar de logging van activiteiten. Met het oog op dat laatste is een project gestart om geautomatiseerde controle hierop plaats te laten vinden.
Voor HPZone (Lite) zijn extra logging functionaliteiten ingericht, is een risicoanalyse uitgevoerd om verdere risico's te identificeren, zijn de aanbevelingen opgepakt en vertaald in een aantal maatregelen, is een project gestart om toegang beter te loggen en monitoren. Naar aanleiding van het onderzoek van RTL zijn onlangs extra maatregelen getroffen om de toegang tot gegevens verder te beperken.
CoronIT heeft geen exportfunctionaliteit. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Het uitzetten van de printfunctionaliteit levert geen problemen op voor het operationeel proces. HPZone heeft zowel een export- als een printfunctionaliteit.De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziektenbestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers.
Met de printfunctionaliteit kan de medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen. De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat alsnog gebeurd. Als gevolg van deze maatregelen kunnen de medewerkers nu minder efficiënt werken.

57. Hoeveel medewerkers zijn inmiddels gecontroleerd en hoeveel onrechtmatigheden zijn inmiddels vastgesteld?

De GGD heeft mij gemeld dat GGD GHOR Nederland op dit moment forensisch onderzoek laat uitvoeren naar de logging (de handelingen die in de GGD-systemen verricht zijn). En tot de start van automatisch en continu monitoren, blijven gespecialiseerde interne en externe teams voor de GGD'en de loggings controleren.

58. Tot slot vragen de leden van de PVV-fractie aandacht voor de mensen van wie data is gelekt. Kan de Minister een inschatting maken hoeveel mensen daadwerkelijk schade zullen ondervinden van deze illegale handel en of deze personen te maken krijgen met identiteitsfraude, bedreigingen of stalking? Zo nee, waarom niet?
Diefstal van persoonsgegevens kan aanleiding geven tot misbruik, bijvoorbeeld voor het plegen van identiteitsfraude. Of en zo ja in welke mate er in het onderhavige geval sprake is (geweest) van misbruik is nog in onderzoek.

59. Kan de Minister achterhalen van hoeveel mensen persoonsgegevens zijn gestolen en/of doorverkocht?
Of en zo ja in welke mate de data zijn verhandeld is nog niet vastgesteld.

60. Is al over nagedacht hoe deze mensen geholpen kunnen worden?
De GGD heeft mij gemeld dat op dit moment onduidelijk is wat de omvang is van het aantal data dat gestolen is. Dat is onderdeel van het politieonderzoek.
De GGD heeft mij gemeld dat wanneer bekend is van welke personen informatie gestolen is, de GGD hen zal informeren. Burgers moeten te allen tijde kunnen vertrouwen dat medische gegevens veilig worden gedeeld en bewaard, juist vanwege het privacygevoelige karakter van deze gegevens. Incidenten als deze zijn zeer ernstig voor de mogelijke slachtoffers, het vertrouwen heeft schade opgelopen en dat betreur ik.

61. Moeten deze mensen conform de privacywetgeving worden geïnformeerd?
In algemene zin staat op de website van GGD GHOR Nederland advies om waakzaam te zijn voor verschillende vormen van cybercriminaliteit. Tevens staat op de website een uitgebreide FAQ, die de komende tijd verder aangevuld zal worden. Als het antwoord op de vraag van personen daar niet tussen staat, kunnen zij contact opnemen met een speciaal ingericht telefoonnummer van GGD GHOR Nederland, dat 7 dagen per week tussen 9.00 uur en 21.00 uur bereikbaar is.

62. Zijn de betrokken personen überhaupt op de hoogte gesteld van de handel in hun data en kunnen zij ergens terecht met vragen hierover?
Voor het antwoord op deze vraag verwijs ik u naar vraag 61.

63. Realiseert de Minister zich dat medische informatie de meest privacygevoelige informatie is die er is? Zo ja, waarom kon dit zo mislopen? Al vele maanden voert de regering campagne die erop gericht is dat mensen zich al met lichte verkoudheidsklachten moeten laten testen.
De verschillende wettelijke waarborgen die er al zijn ten behoeve van de omgang met deze gegevens hebben dit niet kunnen voorkomen. Het is nog te vroeg om exact te duiden hoe dit heeft kunnen gebeuren. Wat er precies is voorgevallen bij de GGD is onderdeel van lopend onderzoek.

64. Wat vindt de Minister ervan dat 7 op 8 personen die een coronatest lieten doen enkel verkouden bleken te zijn en niet besmet met het coronavirus, maar nu wel het slachtoffer kunnen worden van identiteitsfraude? Dit doordat de Minister verantwoordelijk is voor een systeem dat een eitje blijkt te zijn voor diefstal van persoonsgegevens.

Laat ik vooropstellen dat het natuurlijk zeer ernstig is als mensen slachtoffer worden van identiteitsfraude. Het onderzoek van politie en justitie moet vaststellen hoeveel GGD-privégegevens inderdaad verkocht zijn. Ik wil benadrukken dat het belangrijk is dat mensen zich nu niet moeten laten weerhouden om zich te laten testen. Het kan immer bij voorbaat niet gezegd worden dat de klachten die deze mensen hadden «slechts» verkoudheidsklachten waren. Als deze mensen zich dus niet hadden laten testen, hadden ook veel mensen die wél het Coronavirus hadden, zich niet laten testen met alle negatieve gevolgen van dien. Kortom, testen in combinatie met in isolatie gaan wanneer je bent getest is essentieel om te voorkomen dat het virus zich verder verspreid.

Vragen en opmerkingen van de CDA-fractie

De leden van de CDA-fractie maken van de gelegenheid gebruik om enkele vragen te stellen over het datalek bij de coronasystemen van de GGD en de illegale handel in privégegevens als gevolg hiervan.

De GGD gaat geautomatiseerd onderzoeken of medewerkers ongeoorloofd in privégegevens van burgers hebben gekeken. De automatische controle moet eind maart klaar zijn. Tot nu toe vonden dergelijke controles steekproefsgewijs plaats.

65. De leden van de CDA-fractie vragen of de Minister kan aangeven waarom niet vanaf dag één automatische controles zijn ingezet. Hadden deze controles, met bijvoorbeeld de casus waarbij een ziekenhuis een forse boete heeft gekregen van de Autoriteit Persoonsgegevens (AP) in het achterhoofd, niet het uitgangspunt moeten zijn?
De GGD heeft mij gemeld dat bij aanvang van de ontwikkeling en het gebruik van CoronIT het over een substantieel kleinere gebruikersomvang ging. Gedurende de verdere opschaling van het test- en traceerbeleid is de robuustheid en schaalbaarheid van het systeem continu punt van aandacht geweest. Daarbij is een continue afweging gemaakt tussen aanpassingen om beleidswijzigingen te ondersteunen en aan gebruikersvriendelijkheid, bedrijfscontinuïteit en privacy.

66. De leden van de CDA-fractie vragen de Minister welke digitale aanpassingen zijn gedaan aan computers, zodat in het vervolg bijvoorbeeld niet meer gekopieerd kan worden.
Voor het antwoord op deze vraag verwijs ik u naar vraag 17.

67. De leden van de CDA-fractie vragen wat de Minister intussen heeft gedaan om de governance van het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) met betrekking tot ICT aan te passen, naar aanleiding van de onvolkomenheden die de Algemene Rekenkamer in haar onderzoek naar het Jaarverslag 2019 constateerde omtrent het incidentmanagement, het bestuur (governance), de organisatie-inrichting en het risicomanagement.
Naar aanleiding van het rapport van de Algemene Rekenkamer heb ik diverse verbetermaatregelen doorgevoerd. De incidentprocedure is geactualiseerd en er is een nieuwe incidentregistratietool ontwikkeld. Deze tool is door de Algemene Rekenkamer inmiddels als best practice aangemerkt. Ik heb deze tool daarom gedeeld met de andere departementen. Voor wat betreft governance, organisatie inrichting en risicomanagement heb ik het integraal beveiligingsbeleid nader uitgewerkt en zijn de relevante functionarissen structureel met elkaar in contact om ervoor te zorgen dat er niets tussen wal en schip belandt. Daarnaast het ik een plancyclus ingericht waarin beleid en procedures periodiek worden geëvalueerd en geactualiseerd.

68. Welke maatregelen zijn daarnaast genomen op het gebied van archivering, naar aanleiding van de eerdere verdwijning van twee harde schijven uit de kluis met daarop gegevens van het donorregister?
Ik heb aan de Auditdienst Rijk (ADR) gevraagd om onderzoek te doen naar de verdwijning van de harde schijven. In de brief van 6 november 2020 heeft de Minister van MZS (Kamerstuk 32 761, nr. 172) uw Kamer geïnformeerd dat het onderzoek van de ADR vertraging heeft opgelopen en dat de Kamer het onderzoeksrapport inclusief reactie begin 2021 tegemoet kan zien. Het onderzoek van de ADR is inmiddels uitgevoerd en VWS heeft het rapport ontvangen. Ik verwacht dat de Minister voor Medische Zorg en Sport de Kamer in de komende weken zal informeren.

69. In het vragenuur van 26 januari jl. heeft de Minister aangegeven dat «er geen kruid gewassen is» tegen mensen die dit willen doen. De leden van de CDA-fractie vragen of de Minister overleg heeft gehad met bijvoorbeeld telecomproviders die wel in staat zijn strenge maatregelen te nemen ter bescherming van hun netwerk en eveneens niet in de situatie verkeren te kunnen zeggen dat ze niets tegen misbruik kunnen doen? Welke lessen denkt de Minister van hen te kunnen leren?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd (Kamerstukken 27 529 en 32 761, nr. 236).

70. De Minister heeft aangegeven dat zeker 10 duizend GGD-medewerkers de contactgegevens kunnen inzien van mensen die zich hebben laten testen of vaccineren. De leden van de CDA-fractie vragen de Minister waarom duizenden medewerkers data mogen inzien die voor hen niet relevant is. Dat een team verschillende diensten uitvoert is begrijpelijk, maar medewerkers uit bijvoorbeeld Groningen hebben toch niets van doen met gegevens van mensen uit Goes?
De GGD heeft mij gemeld dat bron- en contactmedewerkers van een GGD soms tijdelijk toegang kunnen krijgen tot gegevens van een andere GGD om te ondersteunen bij hoge druk. Verder is er een landelijke schil van BCO-medewerkers. Deze landelijke BCO-medewerkers werken vaak voor meerdere GGD-en en hebben dus toegang tot de gegevens van deze GGD'en. De procedures voor het toegang geven en -na afronding van werkzaamheden- ontnemen, voor landelijke BCO-medewerkers en GGD-medewerkers die ondersteuning hebben geboden bij een andere GGD worden op dit moment door GGD'en kritisch herzien.

71. De leden van de CDA-fractie vragen de Minister welke basissystemen gebruikt worden, van welke leverancier deze systemen zijn, en wanneer deze systemen zijn aangekocht.
De GGD heeft mij gemeld dat HPZone wordt geleverd aan 23 van de 25 GGD'en door het bedrijf inFact sinds 2003. Wijzigingen in HPZone vereisen de instemming van alle partijen, inclusief inFact zelf. HPZone Lite is in gebruik bij alle GGD'en en de landelijke schil voor BCO. CoronIT is in 2020 geleverd aan GGD GHOR Nederland door het bedrijf Topicus.

72. Kan de Minister daarnaast in detail aangegeven welke systemen door de 26 GGD-regio's worden gebruikt, hoe deze aan elkaar zijn gekoppeld, of data bij overdracht zijn versleuteld en zo ja, of dit gebeurt zonder nieuwe versleuteling bij een knooppunt?
De GGD heeft mij gemeld dat het netwerk van gegevensoverdracht onderdeel is geweest van de risico inventarisatie waarover de Tweede Kamer op 24 december 2020 is geïnformeerd. Het is om veiligheidsredenen noch mogelijk noch wenselijk om gedetailleerde informatie te delen over koppelingen en versleutelingen.

73. Welke civielrechtelijke en/of andere juridische stappen worden genomen tegen deze leverancier?
De GGD heeft mij gemeld dat waar nodig de GGD stappen neemt tegen leveranciers op het moment dat niet aan voorwaarden is voldaan en/of de GGD niet in staat wordt gesteld om aan wettelijke vereisten te voldoen.

74. Is deze leverancier alle instructies en voorwaarden van het contract nagekomen met betrekking tot de aanpak van de bescherming van persoonsgegevens of is de leverancier hierin nalatig geweest?
De GGD heeft mij gemeld dat GGD GHOR Nederland een onderzoek instelt of alle instructies en voorwaarden van contracten zijn nagekomen.

75. De leden van de CDA-fractie dachten dat testuitslagen slechts enkele weken bewaard zouden worden. Hoe kan het dan zo zijn dat zo veel data op straat zijn komen te liggen?
De GGD heeft mij gemeld dat op dit moment onduidelijk is wat de omvang is van het aantal data dat gestolen is. Dat is onderdeel van het politieonderzoek.

76. Hoe komt het dat nog niet duidelijk is hoeveel gegevens gestolen zijn?
Zie het antwoord op vraag 75

77. Deze leden vragen verder of er automatische controles zijn omtrent de persoonsgegevens en of in dit kader intussen een extern bureau ingehuurd?
De GGD heeft mij gemeld dat tot de start van automatisch en continu monitoren, gespecialiseerde interne en externe teams voor de GGD'en de loggings blijven controleren.

78. Waarom werd pas in december 2020 een extern bureau ingehuurd om te controleren bij dit proces? Waarom ontbrak de urgentie om de adviezen van dat bureau met spoed te implementeren?
De GGD heeft mij gemeld dat GGD GHOR bezig was met de ontwikkeling van de automatische en continue monitoring. Deze werkzaamheden zijn vertraagd toen de vaccinatie-opdracht versneld bij de GGD'en belegd werd en daarvoor de benodigde functionaliteiten in de systemen ingeregeld dienden te worden. Daarom is het proces van steekproefsgewijze controles destijds voortgezet.

79. De leden van de CDA-fractie vragen de Minister hoe en wanneer burgers van wie de gegevens gestolen zijn,geïnformeerd worden.
De GGD heeft mij gemeld dat wanneer bekend is wie slachtoffer is geworden van datadiefstal, de GGD contact met hen zal opnemen.

80. Deze leden vragen daarnaast hoe burgers hun gegevens uit de systemen van de GGD kunnen laten verwijderen of anonimiseren.
De GGD heeft mij gemeld dat woor het verwijderen of anonimiseren een procedure bestaat via de regionale GGD'en. Hiervoor kan contact worden opgenomen met de regionale GGD.

81. Het blijkt dat ook data van uitgezonden militairen op straat liggen. De leden van de CDA-fractie vragen de Minister welke maatregelen zijn genomen om deze militairen, die in dienst van ons land in gevaarlijke situaties in het buitenland verkeren, te beschermen.
Dit betreft een probleem bij een contractpartner van het Ministerie van Defensie.

82. Volgens RTL heeft de GGD laten weten dat medewerkers een VOG moeten aanleveren en een geheimhoudingsverklaring moeten ondertekenen. De leden van de CDA-fractie vragen de Minister of dit in alle

gevallen tijdens het aannemen van medewerkers is gebeurd, en niet pas nadat medewerkers al enige tijd met de systemen hebben gewerkt.
De GGD heeft mij gemeld dat medewerkers van GGD'en en externe partijen een Verklaring Omtrent het Gedrag (VOG) moeten aanleveren. Gegeven de snelheid waarmee de GGD'en en GGD GHOR Nederland hun personele capaciteit moesten uitbreiden, kunnen zich situaties hebben voorgedaan waarin medewerkers wel toegang hadden tot systemen, maar nog geen VOG hadden overlegd.

83. De leden van de CDA-fractie vragen de Minister of hij kan garanderen dat GGD-medewerkers misstanden intern en desnoods extern kunnen melden zonder dat zij te hoeven vrezen voor represailles.
De GGD geeft aan dat GGD-medewerkers intern misstanden kunnen melden bij vertrouwenspersonen. Zij hoeven niet te vrezen voor represailles.

Vragen en opmerkingen van de D66-fractie

De leden van de D66-fractie zijn verontrust over de illegale handel in grote hoeveelheden gevoelige privégegevens van miljoenen Nederlanders afkomstig uit de slecht beveiligde datasystemen CoronIT en HPzone van de GGD en hebben hierover vragen aan de Minister, in aanloop naar het door de leden van de D66-fractie verzochte Kamerdebat over deze situatie. De leden van de D66-fractie achten het cruciaal dat zorgvuldig met gevoelige gegevens van burgers wordt omgegaan en dat Nederlanders er van verzekerd zijn dat hun gegevens niet in handen van criminelen terecht kunnen komen. Als gevoelige gegevens niet veilig zijn bij de GGD kan dit grote afbreuk doen aan het vertrouwen in de overheid en het draagvlak voor het coronatestbeleid. De leden van de D66-fractie hebben achtereenvolgens vragen en opmerkingen over de inhoud en opbouw van de datasets, de bronnen voor de datasets, de toegang tot de datasets, de beveiliging van de systemen, de risico's voor burgers en overige zaken.

84. De leden van de D66-fractie horen graag van de Minister welke gegevens nu precies per persoon worden vastgelegd en waarom. Waarom zou de GGD bijvoorbeeld het BSN en het adres bewaren van mensen die een coronatest hebben laten doen? Volstaat contactinformatie zoals een telefoonnummer of e-mailadres daarvoor niet?
De GGD heeft mij gemeld dat volledige persoonsgegevens nodig zijn, zodat zeker is dat een test- of vaccinatieafspraak met de juiste persoon wordt gemaakt. Het gebruik van het BSN is noodzakelijk voor de controle van de identiteit. BSN is daarnaast belangrijk, zodat in CoronIT automatisch de juiste persoonsgegevens geregistreerd worden in plaats van dat alle persoonsgegevens handmatig ingevoerd moeten worden (met het risico op administratieve fouten). Daarnaast is het BSN gekoppeld aan DigiD, wat het mogelijk maakt om de uitslag online in te zien. Het woonadres is nodig, zodat we de uitslag ook per brief kunnen toesturen indien er onverhoopt een verkeerd telefoonnummer is geregistreerd en daardoor iemand de uitslag niet heeft kunnen ontvangen.

85. Is het bewaren van grote hoeveelheden gevoelige gegevens wel proportioneel?
De GGD heeft mij gemeld dat voor het plannen van testen, het uitvoeren van bron- en contactonderzoek en het maken van vaccinatieafspraken het bewaren van gevoelige gegevens nodig is.

86. Is bij de ontwikkeling van de systemen gebruik gemaakt van belangrijke principes als privacy by design, dataminimalisatie en doelbinding?
De GGD heeft mij gemeld dat bij de ontwikkeling van CoronIT in 2020 gebruik is gemaakt van de principes die de D66-fractie benoemt. Bij de

ontwikkeling van HPZone dat in 2003 in gebruik is genomen was dat niet het geval.

87. De leden van de D66-fractie vernemen graag hoe de omvangrijke datasets in de systemen nu precies tot stand komen en op basis van welke bronnen ze worden samengesteld. Waar komen de gegevens vandaan?
De GGD heeft mij gemeld dat de gegevens beschikbaar komen bij de registratie van het testen en vaccineren van mensen en uit het bron- en contactonderzoek.

88. Wie leveren een bijdrage aan de datasets?
De GGD heeft mij gemeld dat individuele personen die getest of gevaccineerd worden, of personen die onderdeel zijn van een bron- en contactonderzoek de gegevens die worden verwerkt leveren.

89. Met welke private externe organisaties heeft de GGD samengewerkt voor de totstandkoming van de coronasystemen en de datasets?
De GGD heeft mij gemeld dat HPZone wordt geleverd aan 23 van de 25 GGD'en door het bedrijf inFact sinds 2003. Wijzigingen in HPZone vereisen de instemming van alle partijen, inclusief inFact zelf. HPZone Lite is in gebruik bij alle GGD-en en de landelijke schil voor BCO. CoronIT is in 2020 geleverd aan GGD GHOR Nederland door het bedrijf Topicus

90. Ook vernemen de leden van de D66-fractie graag van de Minister hoe de autorisatie en toegang tot de coronasystemen is geregeld. Welke private externe organisaties hebben er naast de GGD-medewerkers allemaal toegang tot de datasets met gevoelige gegevens?
De GGD heeft mij gemeld dat medewerkers van bedrijven die gecontracteerd zijn voor testen, bron- en contactonderzoek en vaccineren voor de uitoefening van hun werk toegang tot gevoelige gegevens hebben.

91. Hoeveel mensen kunnen in totaal bij deze gegevens?
De GGD heeft mij gemeld dat in totaal bij de 25 regionale GGD'en, GGD GHOR Nederland en gecontracteerde partijen ruim 26.000 mensen betrokken zijn bij testen en vaccineren en ruim 20.000 bij bron- en contactonderzoek.

92. Op welke wijze verliep de autorisatie?
De GGD heeft mij gemeld dat in CoronIT de autorisatie via de daarvoor opgestelde autorisatiematrix verloopt. In HPZone worden rollen toegekend door GGD'en waaraan autorisaties gekoppeld zijn.

93. Hoe werden de gegevens tussen de groep(en) mensen met toegang precies gedeeld? Verliep dat volgens Algemene verordening Gegevensbescherming (AVG)-bestendige normen en protocollen?
De GGD heeft mij gemeld dat gegevens toegankelijk werden gemaakt op basis van de werkverdeling in het kader van bron- en contactonderzoek, testen of vaccineren. Hierbij kunnen meerdere medewerkers toegang hebben tot hetzelfde dossier, omdat dit voor de uitvoering van de werkzaamheden noodzakelijk is. Inmiddels is duidelijk dat de toekenning van rechten te ruim was.

94. Was ook iedereen bij de betrokken private externe organisaties verplicht om een VOG aan te leveren?
De GGD heeft mij gemeld dat medewerkers van GGD'en en externe partijen een Verklaring Omtrent het Gedrag (VOG) moeten aanleveren. Gegeven de snelheid waarmee de GGD'en en GGD GHOR Nederland hun personele capaciteit moesten uitbreiden, kunnen zich situaties hebben voorgedaan waarin medewerkers wel toegang hadden tot systemen, maar nog geen VOG hadden overlegd. Het exacte aantal is niet bekend.

95. Hoeveel mensen hadden toegang tot de coronasystemen zonder een VOG te overleggen?
Voor het antwoord op deze vraag verwijs ik u naar vraag 94.

96. Werd er goed vastgelegd wie op welk moment toegang had tot persoonsgegevens?
De GGD heeft mij gemeld dat logging plaatsvindt. GGD GHOR Nederland laat op dit moment forensisch onderzoek naar de logging (de handelingen die in de GGD-systemen verricht zijn) uitvoeren. Tot de start van automatisch en continu monitoren, blijven gespecialiseerde interne en externe teams voor de GGD'en de loggings controleren.

97. De leden van de D66-fractie willen graag precies van de Minister weten hoe de beveiliging van de systemen en datasets georganiseerd is en met welke waarborgen. Welke controles werden uitgevoerd om de databescherming van miljoenen burgers te waarborgen?
De GGD heeft mij gemeld dat tot nu toe steekproefsgewijze controle van de logging heeft plaatsgevonden.

98. Is na de berichtgeving van de afgelopen dagen centraal en gestructureerd ingegrepen om dit veilig(er) te laten verlopen?
De GGD heeft mij gemeld dat op dit moment forensisch onderzoek plaatsvindt naar de logging (de handelingen die in de GGD-systemen verricht zijn). En tot de start van automatisch en continu monitoren, blijven deze gespecialiseerde interne en externe teams voor de GGD'en de loggings controleren. CoronIT heeft geen exportfunctionaliteit. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Het uitzetten van de printfunctionaliteit levert geen problemen op voor het operationeel proces. HPZone heeft zowel een export- als een printfunctionaliteit. De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziektenbestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers. Met de printfunctionaliteit kan de medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen. De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat alsnog gebeurd. Als gevolg van deze maatregelen kunnen de medewerkers nu minder efficiënt werken.

99. De leden van de D66-fractie vragen ook aandacht voor het volgende. Het uitlekken van (bijzondere) persoonsgegevens zoals BSN's en woonadressen kan grote risico's als identiteitsfraude, intimidatie en stalken meebrengen voor mensen die in de systemen zijn opgenomen. De leden van de D66-fractie horen graag van de Minister of het mogelijk is om persoonsgegevens uit de systemen van de GGD te laten verwijderen? Zo ja, hoe worden mensen hiervan op de hoogte gebracht?
De GGD heeft mij gemeld dat voor het verwijderen of anonimiseren een procedure via de regionale GGD'en bestaat. Hiervoor kan contact worden opgenomen met de regionale GGD. Er is momenteel een extra juridische check gaande om te kijken hoe de wettelijke bewaarplicht zich verhoudt tot de privacy-vraagstukken.

100. Hoe worden slachtoffers geïnformeerd over de vraag of hun gegevens zijn gestolen en/of doorverkocht?
De GGD heeft mij gemeld dat op dit moment onduidelijk is wat de omvang is van het aantal data dat gestolen is. Dat is onderdeel van het politieonderzoek.
De GGD heeft mij gemeld dat wanneer bekend is van welke personen informatie gestolen is, de GGD hen zal informeren. Burgers moeten te alle tijden kunnen vertrouwen dat medische gegevens veilig worden gedeeld en bewaard, juist vanwege het privacygevoelige karakter van deze gegevens. Incidenten als deze zijn zeer ernstig voor de mogelijke slachtoffers, het vertrouwen heeft schade opgelopen en dat betreur ik.

101. Hoe gaat de GGD volgens de Minister communiceren met bezorgde burgers die overwegen geen coronatest meer te doen?
GGD GHOR Nederland heeft mij gemeld dat zij op 29 januari 2021 actief gaan communiceren over de achtergronden van de datadiefstal, de maatregelen die genomen zijn en genomen worden. In die communicatie benadrukt GGD GHOR Nederland het belang van testen én vaccineren.

102. De leden van de D66-fractie horen graag van Minister welke stappen zijn gezet ten behoeve van de informatiebeveiliging van de coronasystemen na de onthulling in september 2020 van Nieuwsuur dat honderden medewerkers van de coronatestlijn ongewenste toegang hadden tot persoonsgegevens. De Minister meldde toen dat er ook sprake was van steekproeven om te controleren of niet gesjoemeld werd met data. Waarom was er sprake van steekproeven en was er geen bredere controle? Wat waren de uitkomsten van deze steekproeven?
De GGD heeft mij gemeld dat bij de bouw van HPZone en CoronIT de keuze is gemaakt om wel te loggen, maar dit niet automatisch en continu te monitoren. Op basis van steekproeven zijn circa 30 medewerkers ontslagen.

103. Was er vaker sprake van datalekken en/of illegale datahandel met corona-gerelateerde systemen die nog niet bekend zijn gemaakt?
De GGD heeft mij gemeld dat er één signaal formeel is binnen gekomen bij GGD GHOR Nederland van medewerkers, hierop is gereageerd en geacteerd. Dit signaal is binnengekomen op 2 juli 2020 en op 9 juli 2020 is gereageerd. Ik verwijs u ook naar de TK brief van 2 februari, waarin een tijdlijn is opgenomen (Kamerstukken 27 529 en 32 761, nr. 236). De risico-analyse (die ik op 24 december 2020 aan u hebt toegezonden (Kamerstuk 25 295, nr. 843)) heeft kwetsbaarheden blootgelegd in de ICT van de GGDen, onder andere op het punt van informatiebeveiliging. De risicoanalyse en de gesprekken daarover hebben helder gemaakt dat het geen gemeengoed was om incidenten onderling te melden aan de partners in de test- en traceerketen (waaronder het Ministerie van VWS). Er is daarom eind december 2020 de afspraak gemaakt dat met onmiddellijke ingang een keten breed incidenten meldingsproces van kracht is geworden. Tot slot: Datalekken die risico's met zich meebrengen voor de betrokken personen moeten door de verantwoordelijke organisatie gemeld worden aan de Autoriteit Persoonsgegevens.

104. Hoe kan het dat grootschalige illegale handel in data afkomstig uit GGD-systemen pas na berichtgeving van RTL op 25 januari jl. naar buiten is gekomen?
De GGD heeft mij gemeld dat hierover nog niet bekend is of er sprake is van grootschalige illegale handel, dit is onderdeel van het onderzoek van politie en justitie.

105. Klopt het dat er zelfs een grootschalige exportfunctie bestond voor data uit de coronasystemen? Zo ja, waarom is hier überhaupt sprake van geweest?
De GGD heeft mij gemeld dat de exportfunctie in HPZone nodig is zodat GGD-epidemiologen analyses en rapportages kunnen maken op basis van datasets. Dat is nodig voor clusteronderzoek en uitbraakbestrijding. Daarnaast is de functie nodig zodat GGD'en analyses kunnen maken ten behoeve van rapportages voor gemeenten in hun GGD-regio.

106. Afgelopen week kwam nog naar buiten dat het bedrijf U-Diagnostics onzorgvuldig om is gegaan met de persoonsgegevens van defensiemedewerkers. Zo zouden (bijzondere) persoonsgegevens van militairen in WhatsApp-groepen gedeeld zijn. De leden van de D66-fractie vragen de Minister of systemen zoals CoronIT, HPzone en andere systemen bij de GGD of het Ministerie van Volksgezondheid op eenzelfde manier tot stand zijn gekomen en op eenzelfde wijze voor grote aantallen mensen toegankelijk zijn.
De GGD GHOR en de GGD'en voeren een eigen beleid bij het ontwikkelen en in gebruik nemen van ICT-systemen. Naast CoronIT en HPzone maken de GGD'en gebruik van andere ICT-systemen die op andere wijze tot stand zijn gekomen. Het Ministerie van VWS maakt gebruik van andere ICT-systemen die op een andere wijze tot stand zijn gekomen.

107. De leden van de D66-fractie vragen de Minister tenslotte waarom niet gebruik is gemaakt van de opgedane ervaring rondom de ontwikkeling van de CoronaMelder, waarbij op een zorgvuldige en intensieve wijze, in samenwerking met veel deskundigen en onderzoekers, veel aandacht is besteed aan informatieveiligheid en privacy by design. Waarom is van deze expertise geen gebruik gemaakt bij CoronIT en HPzone? Zijn deze coronasystemen in tien maanden tijd verbeterd na de ervaring met de CoronaMelder?
De GGD GHOR heeft naar aanleiding van de recente incidenten mijn hulp gevraagd, die ik natuurlijk bereid ben te bieden in de vorm van een expertteam. In dit team zal ook kennis aanwezig zijn over de informatiebeveiliging van CoronaMelder.

108. Is er geregeld contact geweest met de AP over de risico's met betrekking tot de coronasystemen?
N.a.v. de berichtgeving van Nieuwsuur van 16 september jl. is de GGD uitdrukkelijk gewezen op hun wettelijke verplichting te zorgen dat de gegevens van burgers goed beveiligd zijn. De AP heeft aangegeven dat de GGD risico's in kaart moet brengen en waar nodig maatregelen moet treffen om bestaande (en toekomstige) problemen op te lossen. Daarbij is aangegeven dat de AP handhavend kan optreden indien nieuwe signalen/klachten daartoe aanleiding geven.

Vragen en opmerkingen van de GroenLinks-fractie

De leden van de GroenLinks-fractie hebben met grote zorg en verbazing kennisgenomen van het grote datalek bij de digitale coronasystemen van de GGD. Het valt niet genoeg te benadrukken dat het voor het vertrouwen van burgers in de overheid essentieel is dat persoonsgegevens veilig verwerkt worden. In de context van de coronabestrijding is het bovendien van het grootste belang dat mensen zich laten testen bij symptomen en actief deelnemen aan bron- en contactonderzoek. Een datalek bij de digitale coronasystemen van de GGD kan ertoe leiden dat burgers terughoudender worden met het aanvragen van testen en deelnemen aan bron- en contactonderzoek. Dit kan daarmee de coronabestrijding ondermijnen.

109. Wat gaat de Minister in algemene zin doen om het vertrouwen in de systemen van de GGD te herwinnen?
Patiënten moeten ten allen tijde kunnen vertrouwen dat medische gegevens veilig worden gedeeld en bewaard, juist vanwege het privacygevoelige karakter van deze gegevens. Verder verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

110. De leden van de GroenLinks-fractie begrijpen uit de beantwoording van mondelinge vragen over dit onderwerp dat de Minister de oorzaak van dit lek vooral zoekt bij de criminele daden van afzonderlijke medewerkers en niet bij de systeembeveiliging. Kan de Minister deze zienswijze verder toelichten?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

111. Genoemde leden zijn immers van mening dat er wel degelijk veel te verbeteren valt aan de systemen. De Minister stelt dat medewerkers van de GGD alleen toegang hebben tot persoonsgegevens wanneer dit noodzakelijk is voor het uitvoeren van hun werkzaamheden.
Geldt dit ook voor medewerkers van callcenters die in opdracht van de GGD werken?
De GGD heeft mij gemeld dat ook medewerkers van callcenters die in opdracht van de GGD werken toegang hebben tot persoonsgegevens. Dat is noodzakelijk om bijvoorbeeld afspraken te kunnen maken voor testen en vaccineren.

112. Kan de Minister gedetailleerd uiteenzetten tot welke gegevens een medewerker van een callcenter, die belast is met het inboeken van testafspraken en doorbellen van testresultaten, toegang heeft?
De GGD heeft mij gemeld dat in CoronIT naam, adres, woonplaats, telefoonnummer/e-mailadres, BSN, geslacht, geboortedatum, test- en/of vaccineerafspraken en testresultaten staan. Contra-indicaties en COVID-19 klachten. In HPZone staan naam, adres, woonplaats, telefoonnummer, geslacht, geboortedatum en BSN van een persoon. Verder wordt in HPZone ook de informatie uit de bron- en contactonderzoek gesprekken vastgelegd. Dit zijn onder andere: gegevens over COVID-19-gerelateerde klachten/symptomen en huisarts, waar iemand is geweest en met wie hij/zij in contact is geweest. Ook wordt informatie vastgelegd van bron(nen) en nauwe contacten. De gegevens zoals geregistreerd in CoronIT zijn opgenomen in de privacyverklaring CoronIT. Hetzelfde geldt voor HPZone, deze zijn terug te vinden in de privacyverklaring van bron- en contactonderzoek in het kader van COVID-19.

113. Klopt het dat betreffende medewerker toegang heeft tot alle dossiers en niet enkel tot het dossier waar de medewerker op dat moment mee bezig is? Waarom is het noodzakelijk dat een callcentermedewerker toegang heeft tot alle dossiers?
Ik verwijs u naar het antwoord op vraag 30.

114. Is het systeem dusdanig vorm te geven dat een medewerker enkel toegang heeft tot het dossier waar hij of zij op dat moment mee bezig is, en in geen geval toegang heeft tot dossiers die niet door hem of haar op die dag worden behandeld? Zo ja, waarom zijn de systemen dan niet vanaf het begin op deze wijze vormgegeven?
De GGD heeft mij gemeld dat systemen vanaf de aanvang van de pandemie voortdurend aan verandering onderhevig zijn geweest. Er wordt gewerkt aan het verder beperken van zoekfunctionaliteit in CoronIT. Ten behoeve van de ondersteuning van bron- en contactonderzoek wordt zo spoedig mogelijk, een nieuwe applicatie geïntroduceerd waarbij de

bron- en contactonderzoeker alleen toegang heeft tot de dossiers die onder zijn / haar verantwoordelijkheid vallen.

115. Kan de Minister aangeven welke partijen de digitale coronasystemen hebben ontworpen en welke opdrachten daarbij zijn meegegeven vanuit het Ministerie van VWS en vanuit de GGD? Was volledige inachtneming van het principe van privacy by design daar een onderdeel van?
De GGD heeft mij gemeld dat HPZone geleverd wordt aan 23 van de 25 GGD'en door het bedrijf inFact sinds 2003. Wijzigingen in HPZone vereisen de instemming van alle partijen, inclusief inFact zelf. HPZone Lite is in gebruik bij alle GGD-en en de landelijke schil voor BCO. CoronIT is in 2020 geleverd aan GGD GHOR Nederland door het bedrijf Topicus. Privacy en security by design was geen uitgangspunt bij de bouw van HPZone in 2003; wel bij de bouw van CoronIT in 2020.

116. Kunt u voor de systemen CoronIT, HPZone Light en het digitale systeem voor vaccinaties exact aangeven hoeveel mensen toegang hebben tot de gegevens in persoonlijke dossiers? In hoeverre zijn die toegangsrechten al teruggeschroefd? Hoeveel mensen hadden voor die tijd recht op toegang?
De GGD heeft mij gemeld dat in totaal bij de 25 regionale GGD'en, GGD GHOR Nederland en gecontracteerde partijen ruim 26.000 mensen betrokken bij testen en vaccineren zijn en ruim 20.000 bij bron- en contactonderzoek. Toegangsrechten voor een aantal functionaliteiten (met name de export- en printfunctionaliteiten) zijn inmiddels sterk beperkt.

117. Verder vragen de leden van de GroenLinks-fractie de Minister of een callcentermedewerker de mogelijkheid heeft om de gehele database van dossiers te doorzoeken? Zo ja, op welke variabelen kan men dan zoeken? Waarom is dit noodzakelijk voor het uitvoeren van hun werkzaamheden?
Ik verwijs u naar het antwoord op vraag 30

118. Is de Minister bereid om deze zoekfunctie met onmiddellijke ingang stop te zetten?
De GGD heeft mij gemeld dat toegangsrechten voor een aantal functionaliteiten (met name de exportfunctie) inmiddels sterk zijn beperkt. Volledig stopzetten zou betekenen dat medewerkers hun werk niet of niet efficiënt kunnen uitvoeren. Voor CoronIT wordt per 4 februari de zoekfunctie aangepast. Om dossiers terug te vinden zonder het BSN te gebruiken is dan altijd een combinatie van persoonsgegevens noodzakelijk. Onderzocht wordt welke andere maatregelen mogelijk zijn zonder dat dit de effectiviteit van de pandemiebestrijding aantast.

119. De leden van de GroenLinks-fractie zijn ook verbaasd dat callcentermedewerkers toegang hadden tot een exportfunctie waarmee ze gericht konden zoeken naar bepaalde data in de systemen en deze vervolgens grootschalig konden downloaden. Waarom zat deze functie überhaupt in het systeem, zo vragen deze leden aan de Minister? Heeft niemand daar ooit vraagtekens bij geplaatst?
De GGD heeft mij gemeld dat de exportfunctie in HPZone nodig is zodat GGD-epidemiologen analyses en rapportages kunnen maken op basis van datasets. Dat is nodig voor clusteronderzoek en uitbraakbestrijding. Daarnaast is de functie nodig zodat GGD'en analyses kunnen maken ten behoeve van rapportages voor gemeenten in hun GGD-regio.

120. Werkten de callcentermedewerkers met toegang tot deze functie vanuit huis of op kantoor op locatie? In het geval van deze laatste situatie: hoeveel mensen werkten op locatie en beschikten de computers van de callcenters over een geactiveerde USB-poort?

De GGD heeft mij gemeld dat callcenter medewerkers zowel vanuit huis als vanuit kantoor werken. Exacte aantallen zijn niet bekend. Het is niet bekend of (alle) computers van de callcenters over een geactiveerde USB-poort beschikken

121. Kan de Minister garanderen dat medewerkers niet langer de mogelijkheid hebben om data uit de coronasystemen te downloaden en te exporteren?
De GGD heeft mij gemeld dat CoronIT geen exportfunctionaliteit heeft. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Het uitzetten van de printfunctionaliteit levert geen problemen op voor het operationeel proces. HPZone heeft zowel een export- als een printfunctionaliteit.De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziektenbestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers. Met de printfunctionaliteit kan de medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen. De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat alsnog gebeurd. Als gevolg van deze maatregelen kunnen de medewerkers nu minder efficiënt werken.

122. In dit kader vragen de leden van de GroenLinks-fractie de Minister ook om nadere details van de risicoanalyse op de IT-systemen in de test- en traceerketen. De Minister schreef in de Kamerbrief van 24 december jl. (Kamerstuk 25 295, nr. 843) dat naar aanleiding daarvan beter passend autorisatiebeheer zou worden ingericht om het risico op datalekken te minimaliseren. Kan de Minister aangeven hoe dat autorisatiebeheer er voorheen uitzag, welke veranderingen er zouden worden doorgevoerd naar aanleiding van de risicoanalyse en in hoeverre dat al is gebeurd?
De GGD heeft mij gemeld dat autorisatiebeheer per GGD ingeregeld is. GGD'en kennen autorisaties toe aan hun medewerkers en aan medewerkers van gecontracteerde partijen. Naar aanleiding van de risicoanalyse is onder meer actie genomen op het verder definiëren van rollen, welke deels ook afgelopen weken al zijn doorgevoerd.

123. Vormt de recente berichtgeving van RTL over enorme datalekken aanleiding om dat autorisatiebeheer verder aan te scherpen? Zo nee, waarom niet? Zo ja, op welke wijze?
De GGD heeft mij gemeld dat naar aanleiding van de recente berichten de autorisaties voor CoronIT zijn aangepast. Het autorisatiebeheer wordt nog verder aangepast, in HPZone zijn daartoe wijzigingen in de «rollen» van medewerkers aangebracht.

124. Ook vragen deze leden of en zo ja, op welke wijze deze risicoanalyse is gedeeld met de AP. In hoeverre heeft de AP daar kritisch naar kunnen kijken en commentaar op kunnen leveren? Wat is er gebeurd met het commentaar?
De GGD heeft mij gemeld dat de risicoanalyse die genoemd wordt in de Kamerbrief van 24 december niet gedeeld is met de AP.

125. Kan de Minister ook aangeven in hoeverre de digitale coronasystemen in een eerder stadium zijn onderworpen aan een Privacy Impact Assessment of een andere privacy risico-inventarisatie? Wat waren de uitkomsten hiervan, zijn deze gedeeld met de AP en heeft de AP hier kritisch naar kunnen kijken en commentaar op kunnen leveren? Zo ja, wat is daarmee gedaan? Zo nee, waarom niet?
De GGD heeft mij gemeld dat voor CoronIT vanaf het begin en tijdens de ontwikkeling van het systeem een continue risicoanalyse is uitgevoerd, zowel voor testen, het callcenter en vaccineren. Omdat de processen constant onderhevig zijn aan (ad hoc) veranderingen, wordt de risicoanalyse constant bijgehouden en gewijzigd. Het is met andere woorden, een levend document. Daaruit zijn risico's naar boven gekomen, die door de GGD GHOR Nederland of wel zijn gemitigeerd, opgelost, of op basis van een afweging zijn geaccepteerd.
GGD GHOR Nederland heeft de Autoriteit Persoonsgegevens uitgenodigd de continue risicoanalyse gezamenlijk te bespreken.

126. Voorts vragen de leden van de GroenLinks-fractie de Minister of alle data die momenteel wordt verzameld daadwerkelijk noodzakelijk is. Kan de Minister uitleggen waarom de GGD zowel adresgegevens als BSN's nodig heeft?
De GGD heeft mij gemeld dat het registreren van het BSN noodzakelijk is voor de controle van de identiteit. BSN is daarnaast belangrijk, zodat in CoronIT automatisch de juiste persoonsgegevens geregistreerd worden in plaats van dat alle persoonsgegevens handmatig ingevoerd moeten worden (met het risico op administratieve fouten). Daarnaast is het BSN gekoppeld aan DigiD, wat het mogelijk maakt om de uitslag online in te zien. Het woonadres is nodig, zodat de GGD'en de uitslag ook per brief kunnen toesturen indien er onverhoopt een verkeerd telefoonnummer is geregistreerd en daardoor iemand de uitslag niet heeft kunnen ontvangen. Het registreren van het BSN is ook noodzakelijk voor het uitvoeren van het bron- en contactonderzoek.

127. Verwijderen of te laten pseudonimiseren?
De GGD heeft mij gemeld dat voor het verwijderen of anonimiseren een procedure bestaat via de regionale GGD'en. Hiervoor kan contact worden opgenomen met de regionale GGD.

128. De leden van de GroenLinks fractie hoorden de Minister benadrukken dat het kabinet inzet op extra maatregelen om de pakkans te vergroten en dat er meer controles zullen worden uitgevoerd die tevens worden geautomatiseerd. De Minister schreef echter in antwoord op schriftelijke vragen naar aanleiding van een uitzending van Nieuwsuur in september al dat er scherpe controle plaatsvindt op de logging, door nauwlettend bij te houden welke dossiers door wie worden ingezien. Hoe kan het dan dat er toch grootschalig data zijn ingezien en uitgelekt?
De GGD heeft mij gemeld dat steekproefsgewijze logging heeft plaatsgevonden. Het aantal steekproeven zijn na de uitzending van Nieuwsuur opgeschroefd. Daarnaast betreft de exportfunctie een functionaliteit die breed (functioneel) beschikbaar was. Het is nooit helemaal uit te sluiten dat een dergelijke – noodzakelijke – functionaliteit wordt misbruikt en dit is – ook met automatische en continue monitoring – niet 100% uit te sluiten. Inmiddels is de exportfunctie in HPZone uitgeschakeld en zijn er extra loggingsfunctionaliteiten toegevoegd. TVanaf 24 januari en tot de start van automatisch en continu monitoren, blijven zijn gespecialiseerde interne en externe teams voor de GGD'en dagelijks bezig de loggings controleren.

129. Hoe werken die controles precies? Op welk moment gaat er een alarmbel af?

GGD GHOR Nederland laat op dit moment forensisch onderzoek uitvoeren naar de logging (de handelingen die in de GGD-systemen verricht zijn). En tot de start van automatisch en continu monitoren, blijven gespecialiseerde interne en externe teams voor de GGD'en de loggings controleren.

130. Zien de controles enkel toe op toegang tot dossiers, of ook op zoekopdrachten?
De GGD heeft mij gemeld dat de controles toezien op logging (zoekopdrachten en toegang).

131. Kan de Minister aangeven of het klopt dat de GGD alleen steekproefsgewijs controles uitvoert? Zo ja, kan de Minister aangeven waarom dit zo is?
GGD GHOR Nederland heeft mij gemeld op dit moment forensisch onderzoek te laten uitvoeren naar de logging (de handelingen die in de GGD-systemen verricht zijn). En tot de start van automatisch en continu monitoren, blijven gespecialiseerde interne en externe teams voor de GGD'en de loggings controleren.

132. Kan de Minister aangeven of het klopt dat momenteel geen enkele waarschuwing wordt afgegeven, noch aan de medewerker zelf, noch aan de systeembeheerder, wanneer een medewerker een dossier opent waar hij of zij niet aan werkt of een onnodige zoekopdracht uitvoert?
De GGD heeft mij gemeld dat CoronIT en HPZone momenteel nog geen automatisch signaal geven wanneer een medewerker een dossier opent waar hij of zij niet aan werkt of een onnodige zoekopdracht uitvoert. Automatische en continue monitoring wordt voorbereid.

133. Wat waren de bevindingen van de risicoanalyse met betrekking tot de controlesystemen en stonden er ook op dat vlak extra maatregelen gepland? Hoe staat het daarmee?
De GGD heeft mij gemeld dat op basis van een risicoanalyse al extra maatregelen waren gepland. Na de risicoanalyse is een gespecialiseerde externe partij ingeschakeld om het project voor inrichting van geautomatiseerde monitoring te versnellen en extra specialistische kennis toe te voegen om de inrichting van deze monitoring verder vorm te geven.

134. Met betrekking tot de screening van medewerkers geeft de Minister aan dat alle mensen die de GGD aanneemt in bezit moeten zijn van een geldige VOG. Geldt dit ook voor callcentermedewerkers die niet in dienst zijn, maar wel in opdracht van de GGD werken en daarbij toegang hebben tot gevoelige persoonsgegevens? Zo ja, hoe ziet de GGD erop toe dat zijn een VOG overleggen? Zo nee, waarom niet?
De GGD heeft mij gemeld dat ook medewerkers van callcenters een VOG moeten overleggen. In de contracten met de betreffende partijen is dat vastgelegd.

135. Ook vragen de leden van de GroenLinks-fractie de Minister in hoeverre de opsporingsdiensten zich bezighouden met het bestrijden van illegale datahandel?
Het stelen van data en het verhandelen ervan is strafbaar gesteld en het openbaar ministerie treed daar zoals in het onderhavige geval adequaat tegen op. Daarnaast besteden het openbaar ministerie en de politie aandacht aan zogenaamde preventie- en verstoringsmogelijkheden bij specifieke criminele werkwijzen of fenomenen zoals WhatsApp-fraude of hulpvraagfraude of vriend-in-nood-fraude. Daarmee wordt het criminelen zo lastig mogelijk gemaakt om hun activiteiten uit te voeren

136. Hoe is het mogelijk dat de autoriteiten deze grootschalige handel in gegevens uit veelomvattende nieuwe (en dus risicovolle) GGD-systemen

nog niet op het spoor waren en daarop moesten worden gewezen door een journalist?
De GGD-en hebben een eigen verantwoordelijkheid voor de inrichting van de eigen basisbeveiliging. Wanneer er sprake is van een datalek moet hiervan melding worden gemaakt bij de Autoriteit Persoonsgegevens. Daarnaast kan van een vermoeden van datadiefstal (of van een hack) aangifte worden gedaan bij de politie. Het openbaar ministerie heeft naar aanleiding van een melding van mogelijke datadiefstal bij de GGD onmiddellijk actie ondernomen door een opsporingsonderzoek te starten en heeft kort na de start van dit onderzoek twee verdachten aangehouden en voorgeleid

137. Is er zicht op verdere arrestaties van mensen die dit datalek hebben geëxploiteerd? Is daarbij alleen aandacht voor handelaren die de data hebben aangeboden, of gaat men ook op zoek naar individuen die deze illegale datasets hebben gekocht?
Het openbaar ministerie heeft vorige week twee verdachten aangehouden en voorgeleid ter zake van datadiefstal bij de GGD. Uit nader onderzoek moet blijken wie welke rol heeft gehad. Meer aanhoudingen worden niet uitgesloten. Of en zo ja in welke mate de data zijn verhandeld is nog in onderzoek.

138. De leden van de GroenLinks-fractie zijn uitermate bezorgd over de mogelijke gevolgen van het vastgestelde datalek voor de slachtoffers, zoals identiteitsfraude en oplichting. Kan de Minister op deze zorgen ingaan? Welke mogelijke gevolgen ziet de Minister en wat wordt ondernomen om de risico's hiervan te mitigeren?
De zorgen over risico's voor misbruik van gestolen data waarmee vervolgens identiteitsfraude en oplichting kan worden gepleegd zijn begrijpelijk. Het ingestelde opsporingsonderzoek draagt eraan bij dat er beter zicht is of en zo ja welke aanvullende maatregelen nodig zijn.
De GHOR GGD heeft een website https://ggdghor.nl/thema/vragen-antwoorden-datadiefstal/ en telefoonnummer (085–1308266) opengesteld waar bezorgde burgers met vragen terecht kunnen. Hier kunnen vragen worden gesteld over het wel of niet testen zonder risico's; of hun gegevens zijn zijn gestolen en wat ze kunnen doen om mogelijk toekomstige schade te voorkomen. De website verwijst ook naar de relevante websitepagina's van de politie met relevante informatie over beschermingsmaatregelen die mensen kunnen nemen tegen phishing, identiteitsfraude en vriend in nood/Whats app-/ hulpvraagfraude. Slachtoffers van identiteitsfraude kunnen zich melden bij het Centraal Meldpunt Identiteitsfraude of de Fraudehelpdesk. Als burgers daadwerkelijk slachtoffer zijn geworden van fraude met misbruik van persoonsgegevens kunnen ze aangifte doen bij de politie. Als er sprake is van WhatsApp-fraude/ hulpvraagfraude/vriend-in-nood-fraude kan dit online hetgeen versneld mogelijk is gemaakt. Het doen van online aangifte geeft slachtoffers een laagdrempelige mogelijkheid om aangifte te doen, zodat de politie meer inzicht krijgt in de omvang en de aard van deze vorm van criminaliteit. Daarnaast heeft de Minister van Justitie en Veiligheid Uw Kamer geïnformeerd dat de politie is gestart met een landelijke aanpak om deze vorm van oplichting tegen te gaan. De aanpak van WhatsApp-fraude of hulpvraagfraude of vriend-in-nood-fraude wordt daarin centraal opgezet en gecoördineerd. Aangiftes worden landelijk gebundeld, zodat snel zicht ontstaat op zaken die kansrijk zijn en verbanden tussen zaken kunnen worden gesignaleerd. Bij de aanpak wordt nadrukkelijk ook gekeken naar geldezels en criminele samenwerkingsverbanden

139. Deze leden horen zorgwekkende berichten van verschillende GGD'en dat kwetsbare ouderen worden gebeld door mensen die zich voordoen als

GGD-medewerkers en vervolgens worden opgelicht. Hoeveel van deze gevallen zijn bekend bij de regering?
De GGD heeft mij gemeld dat de Fraudehelpdesk heeft aangegeven een tiental meldingen te hebben ontvangen over vermoedelijke oplichters die potentiële slachtoffers telefonisch hebben benaderd en zich uitgaven voor GGD-medewerkers. De Fraudehelpdesk heeft hen geadviseerd om zelf hierover contact op te nemen met de GGD.

140. In hoeverre kunnen deze gevallen van oplichting een verband houden met het datalek bij de GGD?
De GGD heeft mij gemeld dat op dit moment niet met zekerheid vast te stellen is en nog onderdeel van het lopende onderzoek is.

141. Heeft het datalek de kans op dit soort misstanden vergroot?
De GGD heeft mij gemeld dat als vaststaat dat persoonsgegevens zijn verhandeld, wat nog onderdeel is van het lopende onderzoek en nog niet met zekerheid vast te stellen is, het risico (op dit soort misstanden mogelijk zal kunnen vergrotener verschillende maatregelen genomen zijn, waardoor de kans op dit soort misstanden naar de toekomst toe wordt verkleind.

Vanuit de overheid worden er ook publiekscampagnes ingezet om mensen voor te lichten over bewustwording en het bieden van handelingsperspectief in geval van cybercriminaliteit en online fraude. Meer informatie over deze campagnes is te vinden op www.maakhetzieniette-makkelijk.nl en www.veiliginternetten.nl. Op deze websites is ook informatie te vinden over wat men zelf kan doen om deze risico's te verkleinen.

142. In het kader van het mitigeren van de risico's zijn de leden van de GroenLinks-fractie voorts van mening dat het essentieel is om iedereen die mogelijk slachtoffer is geworden van dit datalek daarover zo spoedig mogelijk te informeren, zodat men alert kan zijn op verdachte signalen die kunnen wijzen op misbruik van gestolen persoonsgegevens. Deelt de Minister deze mening en komt hij daarmee ook tot de conclusie dat men daar niet mee kan wachten tot de uitkomsten van strafrechtelijke en forensische onderzoeken bekend zijn? Zo nee, waarom niet? Zo ja, op welke wijze en op welke termijn gaat de Minister de mogelijke slachtoffers informeren?

De GGD heeft mij gemeld dat op dit moment onduidelijk is wat de omvang is van het aantal data dat gestolen is. Dat is onderdeel van het politieonderzoek.
De GGD heeft mij gemeld dat wanneer bekend is van welke personen informatie gestolen is, de GGD hen zal informeren. Burgers moeten te allen tijde kunnen vertrouwen dat medische gegevens veilig worden gedeeld en bewaard, juist vanwege het privacygevoelige karakter van deze gegevens. Incidenten als deze zijn zeer ernstig voor de mogelijke slachtoffers, het vertrouwen heeft schade opgelopen en dat betreur ik.

143. Klopt het dat iedere Nederlander die zich heeft laten testen of is benaderd bij bron- en contactonderzoek mogelijk slachtoffer is?
De GGD heeft mij gemeld dat op dit moment onduidelijk is wat de omvang is van het aantal data dat gestolen is. Dat is onderdeel van het politieonderzoek.

144. Heeft de regering al een idee van het geschatte aantal daadwerkelijke slachtoffers?

De GGD heeft mij gemeld dat op dit moment onduidelijk is wat de omvang is van het aantal data dat gestolen is. Dat is onderdeel van het politieonderzoek.

145 Is de Minister bereid om, in lijn met het advies van de AP, een speciale GGD-informatielijn op te zetten voor bezorgde burgers?
GGD GHOR Nederland heeft mij gemeld dat inmiddels een telefoonnummer geopend waar burgers 7 dagen per week van 9 tot 21 uur terecht kunnen met hun vragen.

146. Deelt de Minister voorts de mening dat wachten met informeren van de mogelijke slachtoffers ook niet in overeenstemming zou zijn met de «Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679» van de Europese Commissie?. Zo nee, kan de Minister dat toelichten onder verwijzing naar Hoofstuk III van de richtsnoeren?
In de richtsnoeren wordt aangegeven dat conform de Algemene verordening gegevensbescherming betrokkenen moeten worden geïnformeerd als een datalek waarschijnlijk een hoog risico voor de rechten en vrijheden van betrokkenen oplevert. De afweging hieromtrent en op welke manier dit gebeurt ligt bij de GGD. De GGD is verwerkingsverantwoordelijke in de zin van de Algemene verordening gegevensbescherming.

Vragen en opmerkingen van de SP-fractie

De leden van de SP-fractie hebben verschillende opmerkingen en vragen over het datalek bij de coronasystemen van de GGD en de vermoedelijke handel in privégegevens van miljoenen Nederlanders uit deze systemen. Zoals op 26 januari jl. tijdens het vragenuur ook is aangegeven, vinden genoemde leden dit een ernstige situatie. Deze leden zijn dan ook van mening dat snelle en complete duidelijkheid essentieel is en dat het vertrouwen onder de Nederlandse bevolking in deze systemen hersteld moet worden.

147. Allereerst vragen de leden van de SP-fractie welke acties zijn genomen nadat Nieuwsuur in september vorig jaar bekend maakte dat honderden testlijnmedewerkers bij alle persoonsgegevens konden, terwijl daar geen noodzaak toe was? Kan chronologisch worden uiteengezet op welk moment welke maatregelen sindsdien zijn genomen om persoonsgegevens beter te beschermen?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

148. Kan de Minister aangeven waarom in het ontwerp van de gebruikte software niet meer maatregelen zijn ingebouwd om persoonsgegevens beter af te schermen?
De GGD heeft mij gemeld dat bij het ontwerp van CoronIT in 2020 security en privacy by design is meegenomen. Bij het ontwerp van HPZone (het systeem dateert uit 2003) niet. Op dit systeem is onder andere een risicoanalyse uitgevoerd om de kwetsbaarheden en risico's te identificeren en te kunnen adresseren (zie vraag 147).

149. Is de mogelijkheid van het (gedeeltelijk) pseudonimiseren van gegevens bij de ontwikkeling van de software overwogen? Waarom is hier niet voor gekozen, denk bijvoorbeeld aan het afschermen van BSN's?
De GGD heeft mij gemeld dat het BSN noodzakelijk is voor de controle van de identiteit, voor de correcte registratie van het persoonsgegevens en om het mogelijk te maken dat geteste personen de uitslag van de test via Digid kunnen inzien.

150. Op welke wijze worden rechten voor het inzien van bepaalde data afgegeven en hoe wordt hierbij voorkomen dat gebruikers meer informatie te zien krijgen dan strikt noodzakelijk is?
De GGD heeft mij gemeld dat HPZone is aangesloten op de centrale autorisatievoorziening. De autorisaties zelf worden toegekend door de GGD'en en ingericht in hun eigen identity provider, die gekoppeld is aan de centrale voorziening. Toekenning van autorisaties gebeurt onder verantwoordelijkheid van de regionale GGD'en. Binnen CoronIT worden lokaal autorisaties toegekend.

151. Hoe kan het dat 26 duizend mensen toegang hebben tot een bestand waarin privacygevoelige informatie van honderdduizenden Nederlanders te vinden is? Zijn hier tijdens het ontwerp en tijdens de ontwikkeling van de software niet al grove fouten gemaakt?
De GGD heeft mij gemeld dat bij aanvang van de ontwikkeling en het gebruik van CoronIT het ging over een substantieel kleinere gebruikersomvang. Gedurende de verdere opschaling van het test- en traceerbeleid is de robuustheid en schaalbaarheid van het systeem continu punt van aandacht geweest. Daarbij is een continue afweging gemaakt tussen aanpassingen om beleidswijzigingen te ondersteunen en aan gebruikersvriendelijkheid, bedrijfscontinuïteit en privacy.

152. Klopt de informatie die de leden van de SP-fractie ter ore is gekomen dat gebruikers van CoronIT of HPZone vergaande aanpassingen kunnen of konden doen in bijvoorbeeld het onderdeel dat de resultaten van het laboratoriumonderzoek weergeeft?
De GGD heeft mij gemeld dat het mogelijk is om in HP Zone laboratoriumgegevens te wijzigen. De reden is dat laboratoriumgegevens deels via beveiligde email binnenkomen en vervolgens handmatig in het systeem worden gezet. Testuitslagen uit GGD teststraten zijn geregistreerd in CoronIT en komen geautomatiseerd in HP Zone binnen via een koppeling. In CoronIT is het voor medewerkers niet mogelijk om resultaten van laboratoriumonderzoek aan te passen

153. Klopt het dat medewerkers die verder niks met het laboratoriumonderzoek te maken hebben gehad op afstand wijzigingen kunnen aanbrengen in het gebruikte afnamemateriaal (swab of speekselspons).
De GGD heeft mij gemeld dat gebruikers die in CoronIT toegang hebben tot het desbetreffende formulier achteraf het gebruikte materiaal kunnen aanpassen op het formulier. Die aanpassing leidt echter niet tot aanpassing in de laborder. In die laborder (de officiële registratie van het onderzoek, zoals die ook aan de laboratoria wordt doorgegeven) blijft het juiste materiaal altijd bewaard.

154. Wat vindt de Minister ervan dat door de GGD en samenwerkende partijen privacygevoelige informatie is uitgewisseld in WhatsAppgroepen? Is dit een veilige manier om informatie te delen en hoe verhoudt zich dit met geldende wet- en regelgeving?
De GGD heeft mij gemeld dat de informatie vooral gedeeld werd vanuit functioneel oogpunt: om collega's snel vooruit te helpen met hun werkzaamheden. Het beleid van de GGD'en is dat het uitwisselen van privacygevoelige informatie via Whatsapp niet toegestaan is.

155. Klopt het dat het oorspronkelijk bedoeld was te communiceren via het programma RocketChat, maar dat dit systeem dusdanig vaak vastloopt dat breed gebruik is gemaakt van WhatsApp? Wat vindt de Minister hiervan?
De GGD heeft mij gemeld dat Rocketchat een communicatieplatform is dat werd gebruikt voor interne communicatie en communicatie tussen callcenteragents onderling bij het call centre om afspraken te maken voor

de teststraat (Teleperformance). Rockchat liep inderdaad zo nu en dan vast. Het gebruik van Whatsappgroepen is door Teleperformance ontmoedigd.

156. Wordt op dit moment wel naar behoren gecommuniceerd?
De GGD heeft mij gemeld dat Rocketchat inmiddels is vervangen door Blackboard.

157. Kan een lijst worden overlegd van de publieke en private organisaties die toegang hebben tot CoronIT en HPZone en aan worden gegeven welke organisaties gemachtigd waren om accounts aan te maken om data te lezen of toe te voegen aan beide systemen?
Organisaties expliciet noemen?
De GGD heeft mij gemeld dat voor HPZone dit de 25 GGD'en en de landelijke callcentra zijn die bij het BCO betrokken zijn (SOS International, Rode Kruis, Eurocross, ANWB, VHD).
Voor CoronIT zijn dit de 25 GGD'en een aantal landelijke partners (Teleperformance, het Rode Kruis, SOS International, Roamler, Unique en Yacht voor het Het Landelijk Serviceloket Testen en tot voor kort de Stichting NLOM van VNOW/NCW).

158. Wie of welke organisatie draagt de eindverantwoordelijkheid voor het geven van rechten aan organisaties voor het werken met beide programma's?
De GGD heeft mij gemeld dat de GGD'en en GGD GHOR Nederland eindverantwoordelijk zijn voor het geven van rechten aan organisaties voor het werken met beide programma's.

159. In de beantwoording op onze eerdergenoemde mondelinge vragen is aangegeven dat RTL de GGD heeft getipt over de illegale datahandel. De leden van de SP-fractie zijn van mening dat dit geen correcte weergave van de werkelijkheid is. Is de Minister het eens met genoemde leden dat RTL kritische vragen heeft gesteld in plaats van dat de GGD door hen is getipt? Zo ja, kan de Minister inzicht geven in de gestelde vragen en antwoorden?
De GGD heeft mij gemeld dat RTL vrijdag 22 januari 2020 contact heeft opgenomen met GGD GHOR Nederland en de organisatie gevraagd te reageren op informatie over datadiefstal. Kritische vragen die terecht gesteld zijn. In reactie op de informatie en de vragen heeft GGD GHOR Nederland onmiddellijk een aantal maatregelen genomen.

160. Kan de Minister in een overzicht aangeven welke wijzigingen aan zowel CoronIT als HPZone zijn aangebracht als gevolg van de vragen die door RTL zijn gesteld? Klopt het bijvoorbeeld dat de exportfunctie, die het grootschalig delen van data een stuk eenvoudiger maakt, pas uitgeschakeld is nadat hier door RTL vragen over zijn gesteld?
De GGD heeft mij gemeld dat zij dit bevestigen. Het is correct dat exportfuncties in HPZone naar aanleiding van de vragen van RTL zijn uitgeschakeld. CoronIT heeft geen exportfunctionaliteit. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Het uitzetten van de printfunctionaliteit levert geen problemen op voor het operationeel proces.
HPZone heeft zowel een export- als een printfunctionaliteit.De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziektenbestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers. Met de printfunctionaliteit kan de

medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen.
De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat alsnog gebeurd. Als gevolg van deze maatregelen kunnen de medewerkers nu minder efficiënt werken. Er worden op dit moment ook andere wijzigingen in de systemen aangebracht. Er wordt gewerkt aan de implementatie van automatische en continue monitoring die eind maart gereed zal zijn. Tot dat moment controleren gespecialiseerde interne en externe teams de logging.

161. De leden van de SP-fractie vragen de Minister om een compleet overzicht in de omvang van het datalek. Indien dit overzicht er niet is, vragen deze leden om een tussenstand en vragen deze leden tevens per wanneer dit overzicht wel volledig beschikbaar is? Daarnaast vragen genoemde leden of dit overzicht direct naar de Kamer gestuurd kan worden wanneer deze gereed is?
De politie doet onderzoek naar welke gegevens gestolen zijn. Het is nu nog onduidelijk welke data er gestolen zijn en om wiens gegevens het gaat.

162. De leden van de SP-fractie krijgen graag een precies overzicht van de ontstane situatie.
Is het bijvoorbeeld duidelijk in welke systemen sprake is van datadiefstal? Is het correct dat dit naast CoronIT ook geldt voor het systeem HPZone, een systeem waar ook medische gegevens worden geregistreerd? Zo ja, welke extra risico's brengt dit volgens de Minister met zich mee en welke specifieke maatregelen worden naar aanleiding hiervan genomen?
De politie doet nog onderzoek naar welke gegevens gestolen zijn. Het is nu nog onduidelijk welke data er gestolen zijn en om wiens gegevens het gaat. CoronIT heeft geen exportfunctionaliteit. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Het uitzetten van de printfunctionaliteit levert geen problemen op voor het operationeel proces.
HPZone heeft zowel een export- als een printfunctionaliteit. De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziekte bestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers. Met de printfunctionaliteit kan de medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen.
De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat alsnog gebeurd. Als gevolg van deze maatregelen kunnen de medewerkers nu minder efficiënt werken.

163. Hoeveel mensen hebben exact toegang tot de persoonsgegevens die zijn opgeslagen in CoronIT? Klopt het dat dit ongeveer 26 duizend mensen

zijn en niet een paar duizend zoals door de Minister werd gesteld tijdens het vragenuur van 26 januari jl.?
De GGD heeft mij gemeld dat het correct is dat circa 26.000 medewerkers toegang hebben tot persoonsgegevens in CoronIT.

164. Hoeveel mensen hebben exact toegang tot de persoonsgegevens die zijn opgeslagen in HPZone?
De GGD heeft mij gedeeld dat circa 20.000 medewerkers toegang hebben tot persoonsgegevens in HPZone (Lite)

165. De leden van de SP-fractie vragen de Minister of gegarandeerd kan worden dat alle medewerkers die toegang hebben tot deze systemen (nu en in het verleden) een VOG en dus geen strafblad hebben?
De GGD heeft mij gemeld dat medewerkers van GGD'en en externe partijen een Verklaring Omtrent het Gedrag (VOG) moeten aanleveren. Gegeven de snelheid waarmee de GGD'en en GGD GHOR Nederland hun personele capaciteit moesten uitbreiden, kunnen zich situaties hebben voorgedaan waarin medewerkers wel toegang hadden tot systemen, maar nog geen VOG hadden overlegd. Het exacte aantal is niet bekend. In totaal zijn bij de 25 regionale GGD'en, GGD GHOR Nederland en gecontracteerde partijen ruim 26.000 mensen betrokken bij testen en vaccineren en ruim 20.000 bij bron- en contactonderzoek. Een exact aantal is niet te geven gezien de aantallen en de verschillende arbeidsrelaties. GGD GHOR Nederland zal de regionale GGD'en en gecontracteerde partijen vragen daarover informatie te geven. De volledige administratie is zo snel als mogelijk – rekening houdend met de doorlooptijden voor de VOG-aanvraag – medio maart op orde.
Een VOG wordt verstrekt op basis van een toetsing op het profiel dat voor de betreffende functie is vastgesteld. Het kan zijn dat betrokkene veroordeeld is voor strafbare feiten die niet relevant zijn voor de functie waarvoor de VOG is aangevraagd.

166. Kan de Minister via een overzicht aangeven hoeveel mensen een VOG hebben overlegd aan de GGD en hoeveel niet? Kan dit ook worden gedaan voor de partners waarmee de GGD samenwerkt of heeft samengewerkt?
GGD GHOR Nederland heeft mij gemeld dat zij de regionale GGD'en en gecontracteerde partijen vragen informatie te geven of alle huidige medewerkers over een VOG beschikken en een geheimhoudingsverklaring hebben getekend.

167. De leden van de SP-fractie zijn van mening dat het betreffende systeem volledig veilig dient te zijn, en hebben hierover ook enkele vragen. In zijn beantwoording van de mondelinge vragen van 26 januari jl. is door de Minister aangegeven dat de GGD sinds de start van de coronapandemie continu de systemen controleert. De leden van de SP-fractie horen graag van de Minister of het klopt dat dit niet het geval blijkt te zijn en dat slechts af en toe een steekproef wordt gedaan.
De GGD heeft mij gemeld dat het correct is dat de logging steekproefsgewijs werd gecontroleerd. Inmiddels controleren gespecialiseerde interne en externe teams voor de GGD'en de loggings, tot de start van automatisch en continu monitoren.

168. Klopt het volgens de Minister dat de GGD pas na de melding RTL heeft nagedacht over continue geautomatiseerde controles?
De GGD heeft mij gemeld dat zij vanaf het begin van de pandemie automatische en continue monitoring hebben overwogen. Bij de ontwikkelingen in de eerste maanden is echter de prioriteit gelegd bij de snelle opschaling van de keten die noodzakelijk was om voldoende mensen te kunnen testen en voldoende bron- en contactonderzoek te

kunnen doen. Na een eerder incident in september vorig jaar is besloten, de monitoring in te richten.
Deze werkzaamheden zijn vertraagd toen de vaccinatie-opdracht versneld bij de GGD'en belegd werd en daarvoor de benodigde functionaliteiten in de systemen ingeregeld dienden te worden. Daarom is het proces van steekproefsgewijze controles destijds voortgezet.

169. Worden zoekopdrachten naar specifieke personen gelogd en gecontroleerd?
De GGD heeft mij gemeld dat zoekopdrachten naar specifieke personen inderdaad worden gelogd en vanaf eind maart automatisch en continu gemonitord. Tot de start van automatisch en continu monitoren, blijven gespecialiseerde interne en externe teams voor de GGD'en de loggings controleren.

170. Is er een waarschuwingsmechanisme van kracht voor het geval de gegevens van bepaalde personen worden opgezocht zonder dat hier noodzaak toe is?
De GGD heeft mij gemeld dat op dit moment handmatige monitoring door gespecialiseerde interne en externe teams plaatsvindt. Automatische en continue monitoring wordt voorbereid.

171. Klopt het volgens de Minister dat CoronIT pas sinds kort aan de NEN-7510-norm voldoet? Hoe is het volgens de Minister mogelijk dat het systeem voldoet aan deze NEN-norm, maar het datalek desondanks niet eerder is opgemerkt?
Het software-platform van Topicus waar CoronIT onderdeel van uitmaakt is volledig gecertificeerd. GGD GHOR Nederland bereidt zich voor op certificering volgens NEN 7510.

172. Deelt de Minister de mening dat meer controles het systeem niet direct veiliger maken, maar dat enkel de pakkans van kwaadwillenden hiermee vergroot wordt?
De leden van de SP-fractie vragen of de Minister de mening deelt dat meer controles het systeem niet direct veiliger maken, maar dat enkel de pakkans van kwaadwillenden hiermee vergroot wordt. Risico's in informatiebeveiliging ontstaan in een samenspel van mens en techniek. Geen enkele maatregel kan op zichzelf een systeem veilig maken. Door een gerichte combinatie van maatregelen gericht op gedrag en systemen zelf kan de kans op misbruik wel zo klein mogelijk gemaakt worden. Controles zijn onderdeel van deze combinatie, om te borgen dat andere maatregelen, bijvoorbeeld ten behoeve van gedrag, ook worden nageleefd. Controles en maatregelen bij onrechtmatige inzage horen bij het palet aan maatregelen.

173. Op welke wijze worden de computersystemen daadwerkelijk veiliger gemaakt? Hoe wordt het vertrouwen in deze systemen hersteld?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

174. De leden van de SP-fractie vinden het ernstig dat mensen misbruik van persoonlijke gegevens (kunnen) maken. Welke maatregelen worden volgens de Minister genomen om de handelaars in persoonsgegevens én de eventuele kopers van deze persoonsgegevens op te sporen?
Het openbaar ministerie heeft naar aanleiding van een melding van mogelijke datadiefstal bij de GGD onmiddellijk actie ondernomen door een opsporingsonderzoek te starten. Over welke maatregelen daarin worden genomen om verdachten op te sporen kan ik geen uitspraken doen.Of en zo ja in welke mate de data zijn verhandeld is nog in onderzoek.

175. Welke acties worden ondernomen om te achterhalen wie in de afgelopen maanden nog meer data uit de GGD-systemen hebben onttrokken?
Voor de acties die zijn ondernomen om te achterhalen wie data uit de GGD-systemen te hebben onttrokken verwijs ik u naar de Kamerbrief.

176. Kan de Minister ook reageren op de uitspraken van de AP en de vele meldingen die zij hebben binnengekregen van burgers die vrezen dat hun gegevens verhandeld zijn?
Ik begrijp de zorgen van deze burgers goed. Dit incident schaadt vertrouwen in een tijd waar burgers daar juist vanuit moeten kunnen gaan. Ik heb geen zicht op de precieze meldingen die de AP zelf heeft binnengekregen.
De AP heeft de laatste week bijna 100 telefoontjes ontvangen van verontruste burgers over de problemen bij de GGD. Ook zijn in die week circa 90 klachten ontvangen van burgers met betrekking tot de verwerking van (hun) persoonsgegevens door de GGD.

177. De leden van de SP-fractie vragen de Minister of het datalek ook gevolgen heeft voor de registratie van vaccinaties? Hoe wordt hier precies mee omgegaan? Hoeveel mensen hebben toegang tot deze gegevens?
Het administratiesysteem CoronIT van de GGD'en wordt zowel voor het testen gebruikt als voor vaccineren. GGD GHOR Nederland meldt mij dat het niet zo is dat alle medewerkers bij alle gegevens in CoronIT kunnen. Door middel van rollen en hieraan gekoppelde rechten wordt toegang verschaft. Iemand die vaccinatieafspraken maakt, kan wel de testgegevens zien omdat dat nodig kan zijn om te bepalen of een persoon gevaccineerd kan worden. Iemand die een testafspraak maakt, kan een vaccinatieafspraak wel zien, maar niet de overige bijbehorende medische gegevens. Ik heb aan GGD-GHOR gevraagd nog eens zeer kritisch tegen het licht te houden wat echt nodig is ten aanzien van deze functionaliteit voor het uitvoeren van testen en vaccineren en mij hierover op korte termijn te berichten. Overigens bevatte CoronIT tot voor kort een printfunctie die gebruikt werd bij noodprocedures. Deze functie is uitgezet.
Daarnaast heb ik in de vorige voortgangsbrief aan uw Kamer gemeld dat het centrale informatiesysteem (Covid-19 vaccinatie informatie- en monitoringssysteem, CIMS) in gebruik is genomen door het RIVM. Het systeem zal gevuld worden vanuit de verschillende decentrale systemen, waaronder dat van de GGD'en. Ik heb aangegeven dat het RIVM een proces heeft ingericht voor het beheer en doorontwikkelen van het landelijk register en het nemen van eventuele aanvullend benodigde informatiebeveiligingsmaatregelen. Dit laatste – de informatieveiligheid – is extra actueel geworden naar aanleiding van de recente gebeurtenissen rondom de beveiliging van het GGD-testsysteem. Aan veilige koppelingen met de decentrale systemen is uitgebreid aandacht besteed, zoals ook in eerdere brieven beschreven. Eind december is in het kader van de Data Protection Impact Assessment zeer uitgebreid onderzoek gedaan, door het RIVM zelf en door externen, naar privacy- en informatiebeveiligingsaspecten van CIMS. Naar aanleiding van deze onderzoeken zijn verdere maatregelen genomen om CIMS te beveiligen. Naar aanleiding van de recente gebeurtenissen bij de GGD'en is nog eens een aanvullende risicoanalyse gevraagd. Het RIVM heeft immers de verantwoordelijkheid voor een grote hoeveelheid bijzondere persoonsgegevens van veel Nederlanders. De gevolgen van eventuele gebreken in de bescherming van deze gegevens zouden eveneens groot zijn. Het RIVM geeft aan dat de kans op een inbreuk zoals bij het GGD-systeem gering is. Dit onder meer omdat slechts een beperkt aantal mensen bij de gegevens kan, er geen export- of printfunctie voor eindgebruikers is, en dat de werkzaamheden van eindgebruikers vanuit een gecontroleerde omgeving (kantoor) gebeuren. Alle activiteiten worden gelogd en gecheckt. De komende

maanden worden de bestaande detectie- en monitoringcapaciteiten verder verbeterd

178. Klopt het dat de Minister eerder heeft gesteld dat medewerkers die testafspraken inplannen niet de mogelijkheid hebben om naar de afspraken voor vaccinaties te kijken, maar dat deze medewerkers wel de ingeplande afspraken voor vaccinaties kunnen zien en zij derhalve kunnen zien of iemand wel of niet gevaccineerd is?
GGD GHOR Nederland meldt mij dat het niet zo is dat alle medewerkers bij alle gegevens in CoronIT kunnen. Door middel van rollen en hieraan gekoppelde rechten wordt toegang verschaft. Iemand die vaccinatieafspraken maakt, kan wel de testgegevens zien omdat dat nodig kan zijn om te bepalen of een persoon gevaccineerd kan worden. Iemand die een testafspraak maakt, kan een vaccinatieafspraak wel zien, maar niet de overige bijbehorende medische gegevens. Ik heb aan GGD-GHOR gevraagd nog eens zeer kritisch tegen het licht te houden wat echt nodig is ten aanzien van deze functionaliteit voor het uitvoeren van testen en vaccineren en mij hierover op korte termijn te berichten. Overigens bevatte CoronIT tot voor kort een printfunctie die gebruikt werd bij noodprocedures. Deze functie is uitgezet.

Vragen en opmerkingen van de Partij voor de Dieren-fractie

De leden van de Partij voor de Dieren-fractie maken zich grote zorgen over de volstrekt gebrekkige omgang met (medische) privégegevens bij de GGD. Daarnaast zijn deze leden verontwaardigd over de onvolledige en incorrecte wijze waarop de Minister de Kamer hier bij het vragenuur van 26 januari jl. over informeerde. De leden van de Partij voor de Dieren-fractie hebben de afgelopen jaren al regelmatig gewezen op de gebrekkige infrastructuur die gebruikt wordt bij de digitalisering van de zorg. Zij zijn daarom ook niet verrast dat het hier is misgegaan. Het belang van privacy en het veilig houden van de (medische) gegevens sneuvelt telkens wanneer andere belangen zich aandienen. De fundamentele fout die gemaakt wordt, is dat het beschermen van privacy gezien wordt als iets wat afgewogen kan worden tegenover andere belangen. De bescherming van medische gegevens en het waarborgen van de privacy zou echter een harde randvoorwaarde moeten zijn. Kan een bepaald systeem daar niet aan voldoen? Dan kan het volgens deze leden in principe niet ingevoerd worden.

179. Kan de Minister bevestigen dat een systeem dat niet ontworpen is vanuit de gedachte om de privacy maximaal te beschermen een slecht systeem is en daarom aangepast of vervangen zou moeten worden?
Het belang van goede privacybescherming van gegevens van burgers staat buiten kijf. Wanneer systemen niet voldoen aan de reeds bestaande strenge wet- en regelgeving dienen deze aangepast te worden.

180. De leden van de Partij voor de Dieren-fractie hebben verschillende vragen en opmerkingen over het concrete voorval bij de GDD. Genoemde leden vinden het zeer verontrustend dat dit zo mis heeft kunnen gaan. Mensen moeten zich kunnen laten testen zonder dat zij zich daarbij zorgen moeten maken of dieven er met hun gegevens vandoor kunnen gaan, met alle zeer kwalijke gevolgen van dien. Hoe gaan we ervoor zorgen dat het niet zo is dat minder mensen zich laten testen de aankomende tijd? Hoe gaan we zo snel mogelijk alle mensen waarvan de gegevens zijn gestolen op de hoogte brengen? Kan de Minister bevestigen dat de GGD nog geen enkel idee heeft van de omvang van het lek en het mogelijke misbruik? Klopt het dat de GGD nog niet eens weet welke systemen kwetsbaar zijn en welke niet? Zo ja, wat is de reactie van de Minister daarop en wat gaat de Minister aan doen?

Ik kan de leden van de PvdD-fractie melden dat op dit moment er een politieonderzoek gaande is omtrent de gestolen persoonsgegevens uit de systemen van de GGD, CoronIT en HPZone. Verder verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

181. De leden van de Partij voor de Dieren-fractie vragen of de Minister kan aangeven of de werkwijze, zoals beschreven in het RTL-artikel, inmiddels onmogelijk is gemaakt? Op welke wijze is ingegrepen in de fysieke infrastructuur van de ICT-systemen? Welke aanpassingen zijn gedaan aan welke specifieke systemen?
De GGD heeft mij gemeld dat CoronIT geen exportfunctionaliteit heeft. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Het uitzetten van de printfunctionaliteit levert geen problemen op voor het operationeel proces. HPZone heeft zowel een export- als een printfunctionaliteit.De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziektenbestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers. Met de printfunctionaliteit kan de medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen.
De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat alsnog gebeurd. Als gevolg van deze maatregelen kunnen de medewerkers nu minder efficiënt werken.

182. Welke andere kwetsbaarheden zijn ontdekt?
De GGD heeft mij gemeld dat kwetsbaarheden vertrouwelijke informatie zijn en kunnen om veiligheidsredenen niet worden gedeeld met de Kamer. Ik verwijs u ook naar mijn brief van 24 december jl. over de risico-analyse.

183. Welke signalen waren er al voor de publicatie van RTL bij de GGD dat de veiligheid van de medische gegevens absoluut niet gewaarborgd kon worden? Wat is er met die signalen gebeurd?
De GGD heeft mij gemeld dat er in 2020 enkele incidenten zijn geweest die zijn onderzocht. Bij dat onderzoek zijn ook externe partijen betrokken geweest. Het onderzoek toen heeft geen aanwijzingen opgeleverd voor grootschalig misbruik. Het onderzoek heeft wel geleid tot het besluit om automatische en continue monitoring in te richten.

184. De leden van de Partij voor de Dieren-fractie vragen de Minister hoe het kan gebeuren dat terwijl de systemen niet op orde zijn de GGD-GHOR op haar website zet; «We zorgen ervoor dat we werken met veilige systemen. We testen dat of we laten dat doen.»[1]
De GGD heeft mij gemeld dat HPZone wordt geleverd aan 23 van de 25 GGD'en door het bedrijf inFact sinds 2003. Wijzigingen in HPZone vereisen de instemming van alle partijen, inclusief inFact zelf. HPZone Lite is in gebruik bij alle GGD-en en de landelijke schil voor BCO. CoronIT is in 2020 geleverd aan GGD GHOR Nederland door het bedrijf Topicus.

[1] GGD GHOR, «Wie werken er met jouw persoonsgegevens?» (https://ggdghor.nl/privacyverklaring-coronit/)

Privacy en security by design was geen uitgangspunt bij de bouw van HPZone in 2003; wel bij de bouw van CoronIT in 2020.

185. Op welke manier is getest of de systemen veilig waren? Wat was dan de uitkomst van die testen? Genoemde leden ontvangen graag deze testresultaten.
De GGD heeft mij gemeld dat er in december 2020 een IT-assessment heeft plaatsgevonden op het IT landschap van de COVID-19-bestrijding door GGD GHOR Nederland. Ik heb uw Kamer hierover per brief geïnformeerd op 24 december 2020. Risicoanalyses bevatten vertrouwelijke informatie en kunnen niet altijd openbaar worden gemaakt vanwege risico's in het kader van de informatiebeveiliging.

186. In het vragenuur gaf de Minister aan dat de beveiliging van de systemen onvoldoende was en nu is aangescherpt. Allereerst zijn de leden van de Partij voor de Dieren-fractie van mening dat de beveiliging slechts de laatste schil om het systeem zou moeten zijn en dat het systeem qua opzet al veel veiliger zou moeten zijn. Genoemde leden hebben ook enkele vragen over de beveiliging. De Minister zei dat deze beveiliging voldoet aan de laatste NEN-norm. Bedoelt de Minister dan alleen de NEN 7510? Of bedoelt de Minister ook de subnorm NEN 7512 aangezien de GGD, het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) en callcenters ook gegevens met elkaar uitwisselen?
De GGD heeft mij gemeld dat het software-platform van Topicus waar CoronIT onderdeel van uitmaakt volledig gecertificeerd is. GGD GHOR Nederland bereidt zich voor op certificering volgens NEN 7510.

187. Over de NEN 7512 merkte de Partij voor de Dieren in 2019 al op dat die onvoldoende veilig is. Een constatering die later door een kamerbrede meerderheid gesteund werd via een motie die verzocht om te kijken of bijvoorbeeld minimaal end-to-end encryptie ingevoerd kon worden. De Minister gaf in reactie op die motie (Kamerstuk 27 529, nr. 246) aan dat in het eerste kwartaal van 2021 de NEN-norm herzien zou zijn. Is dat inmiddels het geval?
Ik kan de leden van de Partij voor de Dieren-fractie melden dat op dit moment de NEN 7512, de norm over informatiebeveiliging bij het uitwisselen van (medische) gegevens, herzien wordt. In die herziening wordt End-to-End encryptie als een van de onderwerpen meegenomen. NEN laat mij weten dat de planning voorziet in publicatie eind 2021.

188. Wanneer is de NEN 7510 voor het laatst herzien?
«Het gaat om de huidige NEN 7512.»

189. Als ook de NEN 7512 hier betrekking heeft en de systemen aan de «laatste NEN-norm» voldoen, om welke norm gaat dat dan? De oude norm waarvan al geconcludeerd was dat die onvoldoende veilig was of de nieuwe die in dit kwartaal klaar zou zijn?
Medewerkers van GGD'en en externe partijen moeten een Verklaring Omtrent het Gedrag (VOG) aanleveren. Gegeven de snelheid waarmee de GGD'en en GGD GHOR Nederland hun personele capaciteit moesten uitbreiden, kunnen zich situaties hebben voorgedaan waarin medewerkers wel toegang hadden tot systemen, maar nog geen VOG hadden overlegd.

190. Klopt de berichtgeving dat een groot aantal medewerkers bij de GGD en de callcenters geen VOG heeft overlegd?
De GGD heeft mij gemeld dat medewerkers van GGD'en en externe partijen een Verklaring Omtrent het Gedrag (VOG) moeten aanleveren. Gegeven de snelheid waarmee de GGD'en en GGD GHOR Nederland hun personele capaciteit moesten uitbreiden, kunnen zich situaties hebben

voorgedaan waarin medewerkers wel toegang hadden tot systemen, maar nog geen VOG hadden overlegd.

191. Kan de Minister aangeven waarom hij dan bij het vragenuur meermaals aangaf dat medewerkers een VOG moeten overleggen? Was hij er niet van op de hoogte dat dit niet gebeurd?
Voor het antwoord op deze vraag verwijs ik u naar vraag 198.

192. Kan de Minister aangeven hoe het kan gebeuren dat er mensen waren die geen VOG konden overleggen en wel een strafblad blijken te hebben, toch toegang kregen tot de medische privégegevens van vele duizenden mensen?
De GGD heeft mij gemeld dat medewerkers van GGD'en en externe partijen een Verklaring Omtrent het Gedrag (VOG) moeten aanleveren. Gegeven de snelheid waarmee de GGD'en en GGD GHOR Nederland hun personele capaciteit moesten uitbreiden, kunnen zich situaties hebben voorgedaan waarin medewerkers wel toegang hadden tot systemen, maar nog geen VOG hadden overlegd. Een VOG wordt verstrekt op basis van een toetsing op het profiel dat voor de betreffende functie is vastgesteld. Het kan zijn dat betrokkene veroordeeld is voor strafbare feiten die niet relevant zijn voor de functie waarvoor de VOG is aangevraagd.

193. Kan de Minister aangeven wat hij bedoelt met de uitspraak «Sinds de start van de pandemie controleert de GGD uiteraard continu het gebruik van de systemen»? Wat wordt bedoeld met het woord «continu»? Is er een vorm van continu toezicht? Zoals het tracken van de handelingen die medewerkers doen? Of is er af en toe een steekproef en vindt deze steekproef met enige continuïteit plaats?
Ik kan de leden van de PvdD-fractie melden dat de GGD'en het gebruik van de systemen CoronIT en HPZone door hun medewerkers controleren. Alleen mensen die voor hun werk inzage moeten hebben in een persoonsdossier, mogen dit dossier inzien. Hierop controleren de GGD'en steekproefsgewijs. Bij niet voor het werk noodzakelijke inzage volgt ontslag en indien nodig aangifte. De GGD'en verwachten eind maart systemen te implementeren die automatisch en continu niet-noodzakelijke toegang controleren, om zo verdacht gedrag op te sporen.

194. Deelt de Minister de mening van de leden van de Partij voor de Dieren-fractie dat steekproeven geen vorm van «continu toezicht» zijn? Zo nee, waarom niet?
Het klopt dat steekproefsgewijs wordt gecontroleerd bij de medewerkers die CoronIT en HPZone gebruiken. Eind maart verwachten de GGD'en systemen te implementeren die automatisch en continu niet noodzakelijke toegang controleren, om zo verdacht gedrag op te sporen. Ik verwijs u verder naar de Kamerbrief voor reflectie op mijn uitspraken.

195. De Minister gaf verder in zijn verweer aan: «De mensen die werken bij de GGD hebben alleen toegang tot persoonsgegevens wanneer dit noodzakelijk is.» Kan de Minister bevestigen dat medewerkers ook wanneer dit niet noodzakelijk was gewoon fysieke toegang tot de systemen hadden? Kan de Minister, indien dit het geval is, aangeven waarom hij de Kamer vertelde dat dit niet zo was?
Alle callcentermedewerkers moeten bij alle dossiers kunnen. De reden is dat niet kan worden voorspeld wie er een bepaalde dag belt voor het maken van een afspraak. Verder zijn er de nodige checks & balances ingeregeld in de werkprocessen. Bovendien heeft de GGD mij gemeld dat medewerkers toegang hebben tot persoonsgegevens in CoronIT nodig om afspraken te kunnen maken voor testen en vaccineren. Zij hebben ook toegang nodig tot persoonsgegevens in HPZone (Lite) om bron- en contactonderzoek te kunnen uitvoeren.

Bron- en contactmedewerkers van een GGD kunnen soms tijdelijk toegang krijgen tot gegevens van een andere GGD om te ondersteunen bij hoge druk. Verder is er een landelijke schil van BCO medewerkers. Deze landelijke BCO medewerkers werken vaak voor meerdere GGD-en en hebben dus toegang tot de gegevens van deze GGD'en. De procedures voor het toegang geven en -na afronding van werkzaamheden- ontnemen, voor landelijke BCO medewerkers en GGD medewerkers die ondersteuning hebben geboden bij een andere GGD worden op dit moment kritisch herzien.

De leden van de Partij voor de Dieren-fractie vragen de Minister in zijn antwoord op bovenstaande vraag niet te verwijzen naar het gegeven dat medewerkers wettelijk gezien geen toegang hadden. Het gaat hier niet om de wettelijke toegang maar de fysieke toegang. Oftewel, de fysieke mogelijkheid om de gegevens in te zien en te downloaden.
Dit punt, het kunnen downloaden van gegevens, is een andere zorg van de leden van de Partij voor de Dieren-fractie.

196. Kan de Minister aangeven welke ICT-systemen die gebruikt worden bij de bestrijding van het coronavirus een zogeheten exportfunctie hebben (gehad)?
De GGD heeft mij gemeld dat CoronIT geen exportfunctie heeft. HPZone heeft wel een exportfunctie.

197. Kan de Minister aangeven hoeveel medewerkers (niet het aantal fte, maar aantal medewerkers) toegang hadden tot elk van de gebruikte systemen?
De GGD heeft mij gemeld dat in totaal bij de 25 regionale GGD'en, GGD GHOR Nederland en gecontracteerde partijen ruim 26.000 mensen betrokken bij testen en vaccineren en ruim 20.000 bij bron- en contactonderzoek zijn.

198. Kan de Minister aangeven hoeveel gegevens/dossiers voor het merendeel van die medewerkers in te zien waren?
De GGD heeft mij gemeld dat in CoronIT medewerkers toegang hebben tot alle dossiers, maar niet tot alle gegevens in die dossiers. Welke gegevens toegankelijk zijn, is afhankelijk van hun rol. De landelijke toegang is noodzakelijk omdat iedereen die in Nederland verblijft kan bellen om een testafspraak maken en vrije keuze heeft voor de locatie waar zij zich willen laten testen. In HPZone hebben medewerkers alleen toegang tot de gegevens uit de regio('s) waarvoor zij op dat moment werkzaam zijn.

199. Kan de Minister via het geven van een getal ook aangeven hoeveel medewerkers toegang hadden tot een exportfunctie?
De GGD heeft mij gemeld dat de exportfunctie van HPZone toegankelijk was voor alle medewerkers. Dat is dichtgezet en nu beperkt tot enkele medewerkers per GGD.

200. Was er enige vorm van toezicht op het gebruik van die exportfunctie (logging)?
De GGD mij gemeld heeft dat tot nu toe vond de controle steekproefsgewijs plaats heeft gevonden. Tot de start van automatisch en continu monitoring, blijven specialistisch interne en externe teams voor de GGD'en de loggings controleren.

201. Kan de Minister aangeven waarom deze exportfunctie was ingevoegd? Welk doel diende deze functie en waarom was de toegang ertoe niet verder beperkt?

De GGD heeft mij gemeld heeft dat Dde exportfunctie in HPZone is nodig is, zodat GGD-epidemiologen rapportages kunnen maken op basis van datasets. Daarnaast is de functie nodig zodat GGD'en analyses kunnen maken ten behoeve van rapportages voor gemeenten in hun GGD-regio. De toegang tot die functie is inmiddels beperkt.

202. Kan de Minister reflecteren op zijn uitspraak: «De GGD heeft uiteraard alles gedaan wat nodig en mogelijk is om de systemen verder te beveiligen»? Staat hij nog altijd achter de bewering dat alles gedaan is wat nodig was?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

Voor de leden van de Partij voor de Dieren-fractie is de inzet van de Minister op dit moment niet voldoende. De Minister geeft aan dat medewerkers alleen toegang tot de systemen hebben wanneer dat noodzakelijk is. Dat is incorrect en niet voldoende gewaarborgd. De Minister kan niet enkel blijven vertrouwen op het goede gedrag van de callcenter- en GGD-medewerkers. Het systeem moet ingericht zijn om ook bij overtredingen of misstanden de privacy van mensen zo goed als mogelijk te waarborgen.

203. Is de Minister bereid te kijken in hoeverre het bestaande systeem en de werkwijze daarvoor kan worden aangepast? Is de Minister bereid te kijken of het systeem en de werkwijze zo kunnen werken dat a) zo min mogelijk medewerkers toegang nodig hebben, b) medewerkers die toegang hebben, toegang hebben tot zo min mogelijk gegevens, c) de toegang expliciet niet mogelijk is wanneer deze ook niet nodig is, d) er een continue controle is op welke gegevens door wie geraadpleegd worden en e) de beveiliging van de systemen op het hoogst denkbare niveau is? Is de Minister bereid deze stappen te nemen? Zo ja, op welke termijn gaat dit lukken?
De GGD heeft mij gemeld heeft dat CoronIT heeft geen exportfunctionaliteit heeft. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Het uitzetten van de printfunctionaliteit levert geen problemen op voor het operationeel proces. HPZone heeft zowel een export- als een printfunctionaliteit.De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziektenbestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers. Met de printfunctionaliteit kan de medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen. De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat alsnog gebeurd. Als gevolg van deze maatregelen kunnen de medewerkers nu minder efficiënt werken.
Tot de start van automatisch en continu monitoring, blijven specialistische interne en externe teams voor de GGD'en de loggings controleren. Ook voor de systemen zelf worden aanvullende maatregelen genomen. Voor CoronIT wordt per 4 februari de zoekfunctie aangepast. Om dossiers terug te vinden zonder het BSN te gebruiken is dan altijd een combinatie van persoonsgegevens noodzakelijk. Onderzocht wordt welke andere

maatregelen mogelijk zijn zonder dat dit de effectiviteit van de pandemiebestrijding aantast.

204. Is de Minister bereid om voor de stappen die genomen moeten worden de kennis en kunde die in het afgelopen jaar werd aangetrokken weer in te zetten?
De GGD GHOR heeft naar aanleiding van de recente incidenten mijn hulp gevraagd, die ik natuurlijk bereid ben te bieden in de vorm van een expertteam. In dit team zal ook kennis aanwezig zijn over de informatiebeveiliging van CoronaMelder.

205. De leden van de Partij voor de Dieren-fractie vragen de Minister verder naar de verantwoordelijkheid voor de verwerking van deze gegevens. De Minister verwees hierbij in de Kamer naar de individuele instellingen. Elke instelling is verantwoordelijk voor haar eigen systemen. Kan de Minister aangeven wie er verantwoordelijk was voor de systemen die hier gebrekkig zijn gebleken? Kan de Minister aangeven op welk moment het zijn verantwoordelijkheid wordt? Hoeveel voorvallen in de zorg moeten er nog zijn voordat eindelijk eens grondig de bezem door alle systemen heen gaat? De voorbeelden zijn legio en de zorg is al jarenlang de sector met de meeste datalekken, blijkt uit de jaarrapportages van de AP.
De verantwoordelijkheid voor de ICT-systemen ligt bij de individuele GGD-en en voor een deel van de systemen bij de GGD GHOR. De GGD'en dragen de verwerkingsverantwoordelijkheid in de zin van de AVG. Dit is en blijft te allen tijde de verantwoordelijkheid van de GGD'en.

206. Op welk moment gaat de Minister beseffen dat er iets fundamenteel mis is en de huidige visie en werkwijze tekortschiet?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

207. Een van de voorbeelden waar het ook niet goed gaat en waar dezelfde problematiek speelt als bij de GGD-systemen is de Corona opt-in. Normaal gesproken moet voor het inzien van medische gegevens expliciete toestemming zijn gegeven. Tijdens de eerste golf van de coronacrisis heeft de Minister dit aangepast. Vanaf dat moment konden de dossiers ook worden ingezien van mensen die niet hebben aangegeven of ze toestemming geven voor de inzage van hun medische dossiers. Daarmee werden 8 miljoen medische dossiers fysiek toegankelijk voor heel veel mensen die daar niets mee te maken hebben. Kan de Minister aangeven waarom deze maatregel, die werd ingesteld toen er noodtenten voor de spoedeisende hulp stonden, nu nog altijd nodig is? Had in de tussentijd geen andere oplossing gevonden kunnen worden?
Deze tijdelijke oplossing is nog steeds nodig. De druk op de zorg is onverminderd groot. Dit maakt dat snelle triage en behandeling op de huisartsenpost en spoedeisende hulp nog steeds van het grootste belang is. Dat maakt het noodzakelijk dat een beperkte set medische kerngegevens van patiënten direct digitaal opvraagbaar is.

208. Is de AP nog altijd akkoord met deze uitzondering?
Dit is inderdaad het geval.

209. Is de Minister bereid de AP opnieuw om een advies te vragen op dit punt? Zo nee, waarom niet?
Ik werk aan een algemene maatregel van bestuur (AMvB) die de Corona Opt-in tijdelijk juridisch zal verankeren. Deze AMvB zal, wanneer deze in werking treedt, in plaats van de huidige gedoogconstructie komen. Een voorstel hiertoe ligt reeds voor advies bij de Autoriteit Persoonsgegevens.

U bent hier door de Minister voor Medische Zorg op 14 december jl. over geïnformeerd (Kamerstuk 27 529, nr. 230).

210. Kan de Minister bevestigen dat, net zoals bij de GGD, bij de Corona opt-in een ongelofelijke hoeveelheid mensen fysiek toegang hebben tot de medische gegevens (meer dan 8 miljoen dossiers) waar zij niets mee van doen hebben?
Het bestaan van de zogenaamde Corona Opt-in is niet te vergelijken met het registratiesysteem bij de GGD'en. Met de Corona Opt-in is het technisch mogelijk voor SEH-zorgverleners en huisartsen om een beperkte set huisartsgegevens van patiënten met of verdacht van COVID-19 op de HAP en SEH te raadplegen na het vragen en verkrijgen van toestemming hiervoor van de patiënt.

211. Kan de Minister bevestigen dat ook hier nauwelijks toezicht is of de inzage in deze gegevens rechtmatig en met toestemming plaatsvindt? Kan de Minister de Kamer laten weten op welke manier nu toezicht gehouden wordt op de raadplegingen en of deze rechtmatig zijn?
Zie antwoord op vraag 212.

212. Is het denkbaar dat ook hier gegevens op verzoek verkocht worden? Welke zekerheid heeft de Minister dat dit niet het geval is?
De medische gegevens die raadpleegbaar zijn via de Corona Opt-in, zijn dat enkel door geautoriseerde zorgprofessionals bij HAP's en SEH's. Dit zijn allen gekwalificeerde zorgprofessionals die in het kader van goede zorg en behandeling deze gegevens nodig achten en aanvullend toestemming dienen te vragen voor raadpleging. Daarbij wordt raadpleging gelogd, en deze loggegevens zijn ook weer inzichtelijk voor patiënten. Daarnaast houdt de zorgaanbieder (HAP/SEH) ook een eigen logging bij. De uitwisseling zelf wordt gemonitord op potentieel misbruik. Daarnaast is het niet mogelijk om de gegevens van meerdere patiënten tegelijk op te vragen.

213. Ziet de Minister de parallel tussen de problematiek bij de GGD, de Corona opt-in en bijvoorbeeld het verhaal waarover NRC schreef op 6 december jl.[2]? Dit zijn allemaal voorbeelden van ICT-systemen in de zorg waarbij de toegang tot medische gegevens veel te ruim is geregeld en het toezicht op de inzage gebrekkig is of ontbreekt.
In beide gevallen hebben de door de organisaties getroffen maatregelen dit niet weten te voorkomen. Zoals hierboven aangegeven bij eerdere vragen van de fractie van de Partij voor de Dieren, is het bestaan van de zogenaamde Corona Opt-in niet te vergelijken met het registratiesysteem bij de GGD of de betreffende systemen bij eerder genoemd ziekenhuis. Gelet op de eerdergenoemde waarborgen die daarbij zijn ingebouwd, zie ik daar geen parallellen.

214. Ziet de Minister in dat het Landelijk Schakelpunt precies dezelfde tekortkoming kent en daarom de welhaast onoplosbare problematiek van de Gespecificeerde Toestemming voortbrengt?
Het Landelijk Schakelpunt is een knooppunt dat zorgverleners met elkaar verbindt en hen in staat stelt om bepaalde medische informatie te raadplegen uit de systemen van andere zorgverleners. Er worden geen medische gegevens in opgeslagen. Twee zaken worden wél vastgelegd in het Landelijk Schakelpunt: de uitdrukkelijke toestemming van burgers om deze medische gegevens te raadplegen en de logging van wie welke medische informatie raadpleegt. De Minister voor Medische Zorg en Sport

[2] NRC Handelsblad, 6 december 2020, «Haar medische gegevens las ze terug in een roman» (https://www.nrc.nl/nieuws/2020/12/06/haar-medische-gegevens-las-ze-terug-in-een-roman-a4022814)

heeft besloten het artikel dat Gespecificeerde Toestemming mogelijk zou maken, niet in werking te laten treden (Kamerstuk 27 529, nr. 219). Er is uiteraard nog steeds uitdrukkelijke toestemming nodig voor de beschikbaarstelling van medische gegevens voor behandelingen. Dit geldt overigens niet alleen voor het landelijk schakelpunt maar voor alle elektronische uitwisselingssystemen zoals bedoeld in de de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz).

215. Is de Minister bereid de huidige plannen voor de (verdere) digitalisering van de zorg op dit moment in ieder geval niet verder door te zetten?
Digitalisering is noodzakelijk om de juiste zorg op de juiste plek mogelijk te maken en in het geval van de crisis, zorg te kunnen blijven leveren. Denk hierbij bijvoorbeeld aan beeldbellen, waardoor nu vormen van niet-acute zorg doorgang kunnen vinden. Overigens spelen bij communicatie tussen zorgverleners per fax, brief, DVD etc. vergelijkbare vraagstukken ten aanzien van privacy en informatiebeveiliging als bij elektronische gegevensuitwisseling.

216. Is de Minister bereid om de omgang met medische gegevens radicaal te gaan herzien vanuit het belang van privacy? Alles minder dan dit is naar de mening van de leden van de Partij voor de Dieren-fractie slechts dweilen terwijl de kraan nog loopt.
Privacy en de omgang met medische gegevens gaan hand in hand. Wanneer systemen niet voldoen aan de reeds bestaande strenge wet- en regelgeving dienen deze systemen aangepast te worden. De Autoriteit Persoonsgegevens houdt vervolgens toezicht op de naleving van de bestaande gegevens. Ik zie geen aanleiding om de omgang met medische gegevens radicaal te herzien. Wanneer systemen niet voldoen aan de reeds bestaande strenge wet- en regelgeving dienen deze aangepast te worden.

Vragen en opmerkingen van de SGP-fractie

De leden van de SGP-fractie maken zich ernstig zorgen over het grote datalek bij de GGD en het feit dat uit journalistiek onderzoek van RTL is gebleken dat er wordt gehandeld in privégegevens van miljoenen Nederlanders. Het lek in CoronIT en HPzone is zeer schadelijk voor de testbereidheid en daarmee in potentie een grote bedreiging voor de coronabestrijding van het kabinet.

Omvang

217. De leden van de SGP-fractie vragen aan de Minister van hoeveel Nederlanders inmiddels persoonsgegevens in CoronIT of HPzone zijn geregistreerd. Kan de Minister de aard en omvang van het datalek gedetailleerd toelichten en daarbij ingaan op welk soort (persoons)gegevens het betreft en om hoeveel mensen het gaat?
De politie doet momenteel nog onderzoek naar welke gegevens gestolen zijn. Het is nu nog onduidelijk welke data er gestolen zijn en om wiens gegevens het gaat. De Kamer wordt geïnformeerd wanneer hier meer duidelijkheid over is.

218. Is er duidelijkheid over welke partijen deze gegevens inmiddels in hun bezit hebben? Zo nee, wanneer wordt hier meer over bekend?
Voor het antwoord op deze vraag verwijs ik u naar vraag 217.

219. Kan zo gedetailleerd mogelijk worden aangeven welke GGD-medewerkers toegang hebben of hadden tot welke informatie en om hoeveel medewerkers het gaat?

De GGD heeft mij gemeld heeft dat de GGD-Medewerkers die betrokken zijn bij testen en vaccineren hebben toegang hebben tot persoonsgegevens in CoronIT. GGD-medewerkers die betrokken zijn bij bron- en contactonderzoek hebben toegang tot HPZone (Lite). Samen met de medewerkers van gecontracteerde partijen gaat het om 26.000 medewerkers die toegang hebben tot CoronIT en 20.000 tot HPZone (Lite).

220. Zijn er naast de GGD-medewerkers nog andere betrokken partijen die toegang hebben (gehad) tot deze systemen?
Voor het antwoord op deze vraag verwijs is u naar vraag 219.

221. Hoe is de toegang tot de systemen beveiligd? Welke waarborgen zijn en worden hiervoor gebruikt?
De GGD heeft mij gemeld dat sinds de zomer van 2020 zijn diverse maatregelen getroffen om het toegangsbeheer te verscherpen en om controles uit te voeren op de toegang tot en het gebruik van persoonsgegevens. Gedurende de gehele periode zijn autorisaties verscherpt, waarbij bij CoronIT in eerste instantie aandacht is uitgegaan naar de scheiding van rollen en inrichting van de rollen, vervolgens naar de logging van activiteiten. Met het oog op dat laatste is een project gestart om geautomatiseerde controle hierop plaats te laten vinden.
Voor HPZone (Lite) zijn extra logging functionaliteiten ingericht, is een risicoanalyse uitgevoerd om verdere risico's te identificeren, zijn de aanbevelingen opgepakt en vertaald in een aantal maatregelen, is een project gestart om toegang beter te loggen en monitoren. Naar aanleiding van het onderzoek van RTL zijn onlangs extra maatregelen getroffen om de toegang tot gegevens verder te beperken. CoronIT heeft enkel een printfunctionaliteit. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Het uitzetten van de printfunctionaliteit levert geen problemen op voor het operationeel proces.
HPZone heeft zowel een export- als een printfunctionaliteit.De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziektenbestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers. Met de printfunctionaliteit kan de medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen.
De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat alsnog gebeurd. Als gevolg van deze maatregelen kunnen de medewerkers nu minder efficiënt werken.

Beveiliging

222. Kan de Minister in een tijdlijn aangeven welke stappen vanaf maart 2020 zijn gezet om de IT-systemen van de GGD te beveiligen en te testen op risico's?
Voor het antwoord op deze vraag verwijs ik u naar vraag 221.

223. Welke controls waren er om dit soort grootschalige data diefstal te voorkomen? Wordt er bijvoorbeeld «gelogd» welke medeweker welke data opvraagt (op deze manier zijn daders te identificeren)?

De GGD heeft mij gemeld dat sinds de zomer van 2020 diverse maatregelen zijn getroffen om het toegangsbeheer te verscherpen en om controles uit te voeren op de toegang tot en het gebruik van persoonsgegevens. Gedurende de gehele periode zijn autorisaties verscherpt, waarbij bij CoronIT in eerste instantie aandacht is uitgegaan naar de scheiding van rollen en inrichting van de rollen, vervolgens naar de logging van activiteiten en is een project gestart om geautomatiseerde controle hierop plaats te laten vinden.
Voor HPZone (Lite) zijn extra logging functionaliteiten ingericht, is een risicoanalyse uitgevoerd om verdere risico's te identificeren, zijn de aanbevelingen opgepakt en vertaald in een aantal maatregelen, is een project gestart om toegang beter te loggen en monitoren. Naar aanleiding van het onderzoek van RTL zijn onlangs extra maatregelen getroffen om de toegang tot gegevens verder te beperken.

224. Welke mogelijkheden en controls zijn er via systeembeheer om inzichtelijk te maken op welke concrete schaal data exports zijn verzonden via sociale media, Wetransfer en/of Onedrive.
De GGD heeft mij gemeld dat onderzoekers naar aanleiding van de recente berichtgeving actief op zoek zijn naar het aanbod van gegevens uit CoronIT of HPZOne (Lite) data op het web. Forensisch onderzoek naar de logging gegevens vindt momenteel plaats. Diverse eerdere keren is melding gemaakt over de werking van de GGD-systemen en van problemen en issues. Hier schijnt beperkt iets mee gedaan te zijn.

225. Welke meldingen zijn gedaan? Waarom is hier in beperkte opvolging aan gegeven?
Voor het antwoord op deze vraag verwijs ik u naar vraag 226.

226. Wie is verantwoordelijk voor de slechte opvolging van deze meldingen?
GGD GHOR Nederland heeft mij gemeld dat de signalen die bij hen terecht zijn gekomen steeds onderzocht en opgevolgd. In het verleden heeft dat onder andere geleid tot het laten onderzoeken van de complete logging van CoronIT, het ontslaan van circa 30 medewerkers en het besluit om automatische en continue controle van de logging in te gaan richten.

Gevolgen

227. De belangrijkste zorg van de leden van de SGP-fractie betreft het uitlekken van gevoelige persoonsgegevens, met name BSN's en woonadressen. Klopt het dat zeer veel mensen toegang hadden tot de meest persoonlijke en vertrouwelijke gegevens, waaronder het BSN, geboortedata, adresgegevens?
De GGD heeft mij gemeld dat in totaal bij de 25 regionale GGD'en, GGD GHOR Nederland en gecontracteerde partijen ruim 26.000 mensen betrokken zijn bij testen en vaccineren en ruim 20.000 bij bron- en contactonderzoek.

228. De leden van de SGP-fractie maken zich zorgen over identiteitsfraude, zeker omdat ook veel oudere Nederlanders zijn getest. Is het zo dat de informatie in de IT-systemen na enige tijd automatisch vervalt of wordt verwijderd?
De GGD heeft mij gemeld dat Dde GGD'en houden zich houden aan de wettelijke termijnen die hiervoor gelden. Zij verwijderen de persoonsgegevens als deze niet langer noodzakelijk zijn, met een maximale bewaartermijn van 5 jaar. De GGD'en bewaren de persoonsgegevens in ieder geval voor de gehele duur van de pandemie.

De GGD heeft een wettelijke bewaarplicht van bepaalde gegevens. Er is momenteel een extra juridische check gaande om te kijken hoe de wettelijke bewaarplicht zich verhoudt tot de privacy-vraagstukken.

229. Is het mogelijk om deze gevoelige informatie uit de systemen te verwijderen?
De GGD heeft mij gemeld dat voor het verwijderen of anonimiseren van gevoelige informatie bestaat een procedure bestaat via de regionale GGD'en. Hiervoor kan contact worden opgenomen met de regionale GGD. Er is momenteel een extra juridische check gaande om te kijken hoe de wettelijke bewaarplicht zich verhoudt tot de privacy-vraagstukken.

230. Wanneer wordt duidelijk of er al sprake is geweest van identiteitsfraude, diefstal of stalking?
Het openbaar ministerie heeft vorige week twee verdachten aangehouden en voorgeleid ter zake van datadiefstal bij de GGD. Uit nader onderzoek moet blijken wie welke rol heeft gehad. Meer aanhoudingen worden niet uitgesloten. Of en zo ja in welke mate de data zijn verhandeld is nog in onderzoek. Slachtoffers van bijvoorbeeld identiteitsfraude of andere strafrechtelijk relevante gedragingen die mogelijk gerelateerd kunnen zijn aan het datalek kunnen aangifte doen bij de politie. Daarnaast kan onder meer identiteitsfraude worden gemeld bij het Centrale Meldpunt Identiteitsfraude of bij de Fraudehelpdesk

231. Welke overige maatregelen zijn nodig? Wordt momenteel overlegd met banken en andere instanties over het aanpassen van hun protocollen voor identiteitsverificatie?
De Minister van Justitie en Veiligheid heeft contact opgenomen met de Nederlandse Vereniging van Banken (NVB) en verzocht om na te gaan of en zo ja, welke passende maatregelen nodig zijn om onder meer mogelijke identiteitsfraude te voorkomen. Ook met andere instanties is contact gezocht om alert te blijven op mogelijke risico's van identiteitsfraude. Verder verwijs ik u naar mijn antwoord op vraag 138.

232. Is er een publiekscampagne nodig met voorlichting over kwetsbaarheden, zodat mensen (waaronder ouderen) minder snel misleid worden?
Publiekscampagnes zijn een nuttig middel om mensen bewust te maken van (online) risico's en hen te voorzien van handelingsperspectief. Onderzoek over veilig online gedrag toont bovendien dat respondenten zich minder veilig gedragen dan zij zelf denken. In dat kader is in 2019 de voorlichtingscampagne «Eerst checken, dan klikken» georganiseerd, waar naast het algemene publiek, onder meer senioren een specifieke doelgroep waren. In 2020 is de campagne «senioren en veiligheid» georganiseerd, die zich mede richtte op bewustwording en het bieden van handelingsperspectief voor ouderen in geval van onder andere phishing en hulpvraagfraude. In april wordt deze campagne voor senioren herhaald, waar aandacht is voor onder andere cybercriminaliteit en online fraude, zoals via spoofing. Meer informatie over deze campagne is te vinden op www.maakhetzieniettemakkelijk.nl. Doorlopend wordt aandacht besteed aan online risico's op www.veiliginternetten.nl. Op deze website is ook informatie te vinden over wat men zelf kan doen om deze risico's te verkleinen.
Een aparte campagne over dit onderwerp wordt niet voorzien. De bestaande informatievoorziening binnen het gehele testproces is met grote zorgvuldigheid tot stand gekomen. Desondanks zal deze nog eens extra geëvalueerd op duidelijkheid en betrouwbaarheid, in het bijzonder voor kwetsbare groepen.

233. Welke mogelijkheden biedt de GGD (en andere instanties die zich met de volksgezondheid bezighouden) aan burgers om te zien welke data de

betreffende instantie van hen heeft? In welke mate is het mogelijk om gegevens te verwijderen en/of te anonimiseren? Ik kan de leden van de SGP fractie wijzen op de verschillende rechten die de patiënt/betrokkene heeft op grond van de WGBO, de AVG en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz). Patiënten hebben onder meer het recht hun medisch dossier in te zien en om correctie, aanvulling, of vernietiging van hun dossier te vragen. In hoeverre een dergelijk verzoek gehonoreerd kan worden is de afweging van de zorgverlener/verwerkingsverantwoordelijke op grond van de omstandigheden van het geval.

234. Is het nodig dat er voor alle Nederlanders een nieuw BSN-nummer wordt aangemaakt, omdat het om miljoenen burgers gaat die de afgelopen maanden zijn getest en totaal onduidelijk is hoeveel persoonsgegevens er inmiddels zijn verhandeld?
De leden van de SGP-fractie vragen of het nodig is om voor alle Nederlanders een nieuw BSN aan te maken. Dat is gelukkig niet nodig. De kans op fraude met alleen het BSN is klein. Ook met een BSN in combinatie met naam, adres en woonplaats kunnen geen bankrekeningen worden geopend of telefoonabonnementen worden afgesloten. Het vervangen van alle burgerservicenummers zou daarnaast een ingrijpende operatie zijn. Zo zouden bijvoorbeeld van rechtswege alle in omloop zijnde reisdocumenten vervallen en diverse wetten moeten worden aangepast. Het BSN speelt een sleutelrol in dienstverlening van de gehele overheid en van organisaties die gerechtigd zijn het nummer te gebruiken. Wijzigen van alle nummers, zal processen ernstig verstoren en de gevolgen voor alle individuele burgers zijn niet te overzien.

235. Welke risico's heeft dit datalek voor de (staats)veiligheid, bijvoorbeeld wanneer blijkt dat persoonsgegevens van politici, militairen, medewerkers van inlichtingendiensten en/of politieagenten openbaar zijn?
Deze vraag ligt op dit moment voor bij de diensten die gaan over de veiligheid van de beroepsgroepen waar u specifiek naar vraagt. Dit zijn de NCTV, het Ministerie van Defensie, AIVD, MIVD en de Nationale Politie.

Transparantie

236. Kan de Minister aangeven of het klopt dat de GGD medewerkers onder druk heeft gezet om geen openheid van zaken te geven, of om niet meer met journalisten te praten?
De GGD heeft mij gemeld dat de GGD'en geen medewerkers onder druk hebben gezet om geen openheid van zaken te geven. In algemene zin wordt van medewerkers gevraagd om contacten met journalisten via de daarvoor beschikbare communicatiemedewerkers te laten lopen.

237. Erkent de Minister dat het in deze situatie cruciaal is om zoveel mogelijk transparantie te geven over wat er is gebeurd en welke risico's er op dit moment zijn?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd en ik verwijs naar de gevraagde stukken en het feitenrelaas.

238. Kan de Minister een anoniem loket opzetten waar GGD-medewerkers hun inzichten kunnen delen?
De GGD ziet geen aanleiding om een anoniem loket op te zetten waar GGD-medewerkers hun inzichten kunnen delen. Binnen de GGD'en en bij de gecontracteerde partijen bestaan mogelijkheden voor medewerkers om eventuele zorgen over de beveiliging van systemen te uiten. Te beginnen bij hun leidinggevenden.

Vragen en opmerkingen van de VVD-fractie

De leden van de VVD-fractie hebben met verontrusting kennisgenomen van de berichtgeving dat de GGD al maanden wist van de privacy problemen. Genoemde leden zijn zeer ontstemd over de nadere berichtgeving over deze kwestie en hebben hierbij de volgende vragen.

239. Op 27 januari jl. stelden deskundigen in de Volkskrant dat uitspraken van de Minister over het GGD-datalek aantoonbaar onjuist waren. De leden van de VVD-fractie vernemen graag een reactie van de Minister op dit artikel.
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

240. Kan de Minister het screeningsprotocol voor bron- en contactonderzoekers met de Kamer delen?
De GGD heeft mij gemeld dat nieuwe bron- en contactonderzoekers een Verklaring Omtrent het Gedrag (VOG) dienen aan te leveren en een geheimhoudingsverklaring ondertekenen. Dit is van toepassing op zowel medewerkers van de GGD'en en van externe partijen.

241. Kan de Minister hierbij ook informatie delen over de training die nieuwe medewerkers krijgen omtrent het veilig en zorgvuldig omgaan met gevoelige gegevens?
De GGD heeft mij gemeld dat Dde callcentermedewerkers worden uitvoerig worden gewezen op de privacy-verplichtingen. Ze tekenen een geheimhoudingsverklaring voordat ze aan de slag gaan en de training volgen. Hierin staat ook informatie over het gebruik van sociale media. Tijdens het on-boardingsprogramma en in de training wordt hierover gesproken. Daar wordt benadrukt dat het maken van afbeeldingen van schermen en het delen hiervan niet is toegestaan. Op verschillende manieren worden medewerkers voorzien van de benodigde informatie en mogelijkheden om vragen te stellen.

242. Zijn het screeningsprotocol en de training voor iedere nieuwe medewerker hetzelfde, ongeacht of een medewerker via een externe partij binnenkomt of direct via de GGD?
De GGD heeft mij gemeld dat nieuwe medewerkers een Verklaring Omtrent het Gedrag (VOG) moeten aanleveren en een geheimhoudingsverklaring ondertekenen. Dit is van toepassing op zowel medewerkers van de GGD'en alsen van externe partijen. De training van de landelijke partners is hetzelfde, per GGD kan echter de training verschillen. De training is voor de start van werkzaamheden en periodiek.

243. Genoemde leden lezen dat de exportfunctie in CoronIT kan worden gebruikt om overzichten met dossiers te exporteren als pdf- of Exceldocument. Deze documenten kunnen doorgestuurd worden. Kan de Minister aangeven waar geëxporteerde overzichten met dossiers voor gebruikt worden?
De GGD heeft mij gemeld dat CoronIT heeft enkel een printfunctionaliteit. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Het uitzetten van de printfunctionaliteit levert geen problemen op voor het operationeel proces. Met de printfunctionaliteit kan de medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen.

HPZone heeft zowel een export- als een printfunctionaliteit. De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziekte bestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers. De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat alsnog gebeurd. Als gevolg van deze maatregelen kunnen de medewerkers minder efficiënt werken.

244. Kan de Minister aangeven of de exportfunctie van zowel CoronIT en HPZone verwijderd is?
Voor het antwoord op deze vraag verwijs ik naar de vraag 243.

245. Welke invloed heeft het verwijderen van de exportfunctie voor de werkzaamheden van de GGD en uitvoering van het bron- en contactonderzoek?
Voor het antwoord op deze vraag verwijs ik naar de vraag 243.

246. Klopt het dat informatie over onderliggende medische aandoeningen en zwangerschappen worden geregistreerd in HPZone? Met welk doel worden deze specifieke gegevens geregistreerd?
De GGD heeft mij gemeld dat zij de GGD is op basis van de Wet op de Geneeskundige Behandelovereenkomst (WGBO) ook verplicht zijn om bepaalde gegevens vast te leggen. Dit zijn onder andere gegevens over COVID-19-gerelateerde klachten/symptomen en huisarts. Deze gegevens worden geregistreerd in het kader van het bron- en contactonderzoek en met het oog op contra-indicaties voor vaccinatie.

247. Kan de Minister exact aangeven welke gegevens van personen worden opgeslagen in HPZone?
In CoronIT staan onder andere naam, adres, woonplaats, telefoonnummer/e-mailadres, BSN, geslacht, geboortedatum, test- en/of vaccineerafspraken en testresultaten. Contra-indicaties en COVID-19 klachten. In HPZone staan naam, adres, woonplaats, telefoonnummer, geslacht, geboortedatum en BSN van een persoon. Verder wordt in HPZone ook de informatie uit de bron- en contactonderzoek gesprekken vastgelegd. Dit zijn onder andere: gegevens over COVID-19-gerelateerde klachten/symptomen en huisarts waar iemand is geweest en met wie hij/zij in contact is geweest.

248. Kunnen dossiers uit HPZone ook geëxporteerd worden?
De GGD heeft mij gemeld dat HPZone zowel een export- als een printfunctionaliteit heeft. De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziekte bestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers. Met de printfunctionaliteit kan de medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen. De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat alsnog gebeurd. Als gevolg

van deze maatregelen kunnen de medewerkers nu minder efficiënt werken.

249. Welke medewerkers hebben toegang tot CoronIT en welke medewerkers tot HPZone?
De GGD heeft mij gemeld dat in totaal bij de 25 regionale GGD'en, GGD GHOR Nederland en gecontracteerde partijen ruim 26.000 mensen betrokken zijn bij testen en vaccineren en ruim 20.000 bij bron- en contactonderzoek.

250. Klopt het dat gevoelige gegevens in CoronIT en HPZone ook «gewijzigd» konden of kunnen worden? Zo ja, door wie en onder welke voorwaarden?
De GGD heeft mij gemeld dat het mogelijk is om in HP Zone laboratoriumgegevens te wijzigen. De reden is dat laboratoriumgegevens deels via beveiligde email binnenkomen en vervolgens handmatig in het systeem worden gezet. Testuitslagen uit GGD teststraten zijn geregistreerd in CoronIT en komen geautomatiseerd in HP Zone binnen via een koppeling. In CoronIT is het voor medewerkers niet mogelijk om resultaten van laboratoriumonderzoek aan te passen.

251. Kan de Minister voorts aangeven of de mogelijkheid bestaat of bestond dat testresultaten «gewijzigd» kunnen of konden worden? Zijn er aanwijzingen dat dit ook gebeurd is?
De GGD heeft mij gemeld dat het mogelijk is om in HP Zone laboratoriumgegevens te wijzigen. De reden is dat laboratoriumgegevens deels via beveiligde email binnenkomen en vervolgens handmatig in het systeem worden gezet. Er zijn geen aanwijzingen dat in al geregistreerde gegevens is gewijzigd.
Dit is de reden waarom GGD GHOR Nederland de afgelopen tijd heeft gewerkt aan koppelingen voor testuitslagen van niet-GGD teststraten. Hierdoor hoeven testuitslagen niet meer handmatig worden ingevoerd. Testuitslagen uit GGD teststraten zijn geregistreerd in CoronIT en komen geautomatiseerd in HP Zone binnen via een koppeling. In CoronIT is het voor medewerkers niet mogelijk om resultaten van laboratoriumonderzoek aan te passen. Er zijn geen aanwijzingen dat in al geregistreerde gegevens is gewijzigd.

252. Van welke GGD-regio's konden bron- en contactonderzoekers, overige medewerkers van de GGD en medewerkers via externe partijen gegevens inzien?
De GGD heeft mij gemeld dat bron- en contactmedewerkers van een GGD soms tijdelijk toegang krijgen tot gegevens van een andere GGD om te ondersteunen bij hoge druk. Verder is er een landelijke schil van BCO medewerkers. Deze landelijke BCO medewerkers werken vaak voor meerdere GGD-en en hebben dus toegang tot de gegevens van deze GGD-en. De procedures voor het toegang geven en -na afronding van werkzaamheden- ontnemen, voor landelijke BCO medewerkers en GGD medewerkers die ondersteuning hebben geboden bij een andere GGD worden op dit moment kritisch herzien. Gezien de maatregelen rondom het coronavirus hebben veel bron- en contactonderzoekers hun werkzaamheden thuis verricht.

253. Kan de Minister beschrijven hoe het inlogproces in HPZone vanuit de thuisomgeving eruitziet?
De GGD heeft mij gemeld dat dat er als volgt uitziet: De gebruiker gaat vanuit zijn browser naar een beveiligde website. Op deze beveiligde website kan de gebruiker inloggen met een gebruikersnaam en wachtwoord en wordt tevens om een extra verificatiecode gevraagd die wordt gegenereerd door een authenticatie app die de gebruiker vooraf heeft

moeten installeren op zijn/haar mobiele telefoon. Nadat de gebruiker met deze gegevens heeft ingelogd, ziet de gebruiker het icoon van HPZone, en kan hij voor toegang klikken op het icoon, en heeft daarmee in basis toegang tot HPZone. Afhankelijk van functie en organisatie (GGD'en en landelijke partners hebben toegang tot aparte delen van HPZone) heeft de gebruiker toegang tot het deel van HPZone waarvoor hij is geautoriseerd.

254. Kan de Minister daarbij tevens aangeven hoe het inlogproces in HPZone in de werkomgeving eruitziet?
De GGD heeft mij gemeld dat dat er als volgt uitziet:Het inloggen van de gebruiker in HPZone is direct gekoppeld aan het inloggen op de onder vraag 253 genoemde beveiligde website. De gebruiker kan binnen HPZone een aantal mogelijke rollen krijgen, die bepalen welke werkzaamheden een gebruiker in de applicatie kan verrichten, en die afhankelijk zijn van zijn/haar functie. Binnen HPZone zijn drie verschillende typen gebruikers. Medewerkers die toegang hebben tot HPZone, medewerkers die toegang hebben tot HPZone Lite en medewerkers van de landelijke partners.
De medewerkers die toegang hebben tot HPZone hebben, afhankelijk van de hen toegekende rollen toegang, tot de data van de GGD waar zij bij horen. De medewerkers die toegang hebben tot HPZone Lite hebben, afhankelijk van de toegekende rollen, beperkte functionaliteit van HPZone van de GGD waar zij bij horen. De medewerkers van de landelijke partners hebben, afhankelijk van de hen toegekende rollen, toegang tot HPZone Lite. Zij hebben géén toegang tot data van een GGD en moeten deze toegang aanvragen bij elke GGD waarvoor zij werkzaamheden moeten verrichten. Nadat de GGD de toegang voor de medewerker van de landelijke partner heeft verricht, heeft deze toegang tot de data van de betreffende GGD. HPZone Lite wordt uitsluitend voor bestrijding van COVID-19 gebruikt.

255. Kan de Minister dit ook aangeven voor CoronIT?
De GGD heeft mij gemeld dat dit voor CoronIT overal hetzelfde is: een medewerker gaat naar de loginpagina van CoronIT en logt daar in met gebruikersnaam en wachtwoord. Die login moet worden bevestigd met een code van een app op de telefoon (Microsoft Authenticator, Google authenticator of een vergelijkbare app). Die code is slechts beperkt geldig. In andere landen, zoals Duitsland, wordt ook op grote schaal bron- en contactonderzoek uitgevoerd.

256. Kan de Minister aangeven met welke systemen hier gewerkt wordt en welke medewerkers toegang hebben tot welke systemen en welke gegevens?
«De GGD heeft mij gemeld dat de VOG wordt gebruikt als screenings-middel. Ook kan ik de leden van de VVD-fractie melden dat bij de GGD'en de calcentermedewerkers uitvoerig worden gewezen op de privacy-verplichtingen. Ze tekenen een geheimhoudingsverklaring voordat ze aan de slag gaan en de training volgen. Hierin staat ook informatie over het gebruik van social media. Tijdens het on-boardingsprogramma en in de training wordt hierover gesproken. Daar wordt benadrukt dat het maken van afbeeldingen van schermen en het delen hiervan niet is toegestaan. Op verschillende manieren worden medewerkers voorzien van de benodigde informatie en mogelijkheden om vragen te stellen. De training van de GGD GHOR Nederland is hetzelfde, per GGD kan echter de training verschillen. De training is voor de start van werkzaamheden en periodiek. Verder is er bij de BCO-schil een systeem van feedback.»

257. Kan de Minister voorts aangeven hoe de screening van nieuwe medewerkers en de training van deze medewerkers over hoe veilig en verantwoord om te gaan met gevoelige informatie eruitziet?

De GGD mij heeft gemeld dat de VOG wordt gebruikt als screeningsmiddel. Ook kan ik de leden van de VVD-fractie melden dat bij de GGD'en de calcentermedewerkers uitvoerig worden gewezen op de privacyverplichtingen. Ze tekenen een geheimhoudingsverklaring voordat ze aan de slag gaan en de training volgen. Hierin staat ook informatie over het gebruik van social media. Tijdens het on-bourdingsprogramma en in de training wordt hierover gesproken. Daar wordt benadrukt dat het maken van afbeeldingen van schermen en het delen hiervan niet is toegestaan. Op verschillende manieren worden medewerkers voorzien van de benodigde informatie en mogelijkheden om vragen te stellen. De training van de GGD GHOR Nederland is hetzelfde, per GGD kan echter de training verschillen. De training is voor de start van werkzaamheden en periodiek. Verder is er bij de BCO-schil een systeem van feedback.

258. Kan de Minister een overzicht met tijdlijn geven van de stappen die hij en de GGD hebben doorlopen om de veiligheid van de systemen van de GGD te borgen?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

Vragen en opmerkingen van de PVV-fractie

De leden van de PVV-fractie hebben met verbazing uit de media vernomen dat de GGD al maanden wist van de privacy problemen rondom de coronasystemen. Genoemde leden vinden het onbegrijpelijk dat de GGD niet direct actie heeft ondernomen, nadat verschillende medewerkers over de privacy kwestie aan de bel hadden getrokken. Deze leden hebben daarom nog de volgende dringende vragen.

259. De leden van de PVV-fractie willen van de Minister weten wanneer de coronasystemen in zijn ingevoerd en of het klopt dat alle gegevens vanaf het begin door iedereen waren in te zien, op te vragen en/of door te sturen?
De GGD heeft mij gemeld dat HPZone geleverd wordt aan 23 van de 25 GGD'en door het bedrijf inFact sinds 2003. Wijzigingen in HPZone vereisen de instemming van alle partijen, inclusief inFact zelf. HPZone Lite is in gebruik bij alle GGD'en en de landelijke schil voor BCO. CoronIT is in 2020 geleverd aan GGD GHOR Nederland door het bedrijf Topicus.
In totaal zijn bij de 25 regionale GGD'en, GGD GHOR Nederland en gecontracteerde partijen ruim 26.000 mensen betrokken bij testen en vaccineren en ruim 20.000 bij bron- en contactonderzoek. Toegangsrechten voor een aantal functionaliteiten (met name de export- en printfunctionaliteiten) zijn inmiddels sterk beperkt

260. Wanneer kwamen de eerste signalen over de onveilige situatie naar boven? Klopt het dat dit medio april 2020 was?
De GGD heeft mij gemeld dat er één signaal formeel is binnen gekomen bij GGD GHOR Nederland van medewerkers, hierop is gereageerd en geacteerd. Dit signaal is binnengekomen op 2 juli 2020 en op 9 juli 2020 is gereageerd. Ik verwijs u ook naar de Kamerbrief van 2 februari, waarin een tijdlijn is opgenomen. De risico-analyse (die ik op 24 december 2020 aan u hebt toegezonden) heeft kwetsbaarheden blootgelegd in de ICT van de GGDen, onder andere op het punt van informatiebeveiliging. De risicoanalyse en de gesprekken daarover hebben helder gemaakt dat het geen gemeengoed was om incidenten onderling te melden aan de partners in de test- en traceerketen (waaronder het Ministerie van VWS). Er is daarom eind december 2020 de afspraak gemaakt dat met onmiddellijke ingang een keten breed incidenten meldingsproces van kracht is geworden. Tot slot: Datalekken die risico's met zich meebrengen voor de

betrokken personen moeten door de verantwoordelijke organisatie gemeld worden aan de Autoriteit Persoonsgegevens.

261. Wat is er wanneer met deze signalen gedaan?
Voor het antwoord op deze vraag verwijs ik naar vraag 260.

262. Hoeveel meldingen over de problemen zijn in totaal binnengekomen?
Voor het antwoord op deze vraag verwijs ik naar vraag 260.

263. Hoeveel leidinggevenden waren op de hoogte van de meldingen?
De GGD heeft mij gemeld dat het onbekend is of de leidinggevende over de melding geïnformeerd is.

264. Werd de voorzitter van de koepelvereniging GGD GHOR hierover geïnformeerd? Zo ja, wanneer? Zo nee, waarom niet?
De GGD heeft mij gemeld dat het niet bekend is of de vorige voorzitter is geïnformeerd. Eind oktober is de huidige voorzitter op hoofdlijnen geïnformeerd over zwakheden in systeem (continuïteit, betrouwbaarheid en veiligheid) en het ingezette verbeterplan.

265. Werd de Minister hier zelf over geïnformeerd? Zo ja, wanneer? Zo nee, waarom niet?
Ik ben daar niet over geïnformeerd. Voor het antwoord op deze vraag verwijs ik naar vraag 260.

266. Werden ambtenaren op het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) hierover geïnformeerd? Zo ja, wanneer? Zo nee, waarom niet?
Voor het antwoord op deze vraag verwijs ik naar vraag 260.

267. De leden van de PVV-fractie begrijpen niet hoe het kan dat de onveilige datasituatie zo lang bleef bestaan. Wie besloot, wanneer en op basis waarvan dat het akkoord was om de onveilige privacy situatie te laten voortduren?
De GGD heeft mij gemeld dat bij aanvang van de ontwikkeling en het gebruik van CoronIT het over een substantieel kleinere gebruikersomvang ging. Gedurende de verdere opschaling van het test- en traceerbeleid is de robuustheid en schaalbaarheid van het systeem continu punt van aandacht geweest. Daarbij is een continue afweging gemaakt tussen aanpassingen om beleidswijzigingen te ondersteunen en aan gebruikersvriendelijkheid, bedrijfscontinuïteit en privacy. Voor HPZone geldt dat individuele GGD'en een contract hebben met de leverancier en dit niet centraal in één hand ligt. Er is meermalen getracht deze situatie te veranderen en afspraken te maken met de leverancier. Het doorvoeren van maatregelen bleef gecompliceerd en daarom is besloten te starten met het ontwikkelen van een nieuw systeem en over te gaan zodra mogelijk.

268. Is op enig moment overwogen over te gaan op een systeem waarbij géén Burgerservicenummer (BSN) meer werd gevraagd? Zo ja, wanneer? Zo nee, waarom niet?
De GGD heeft mij gemeld dat volledige persoonsgegevens nodig zijn, zodat zeker is dat een test- of vaccinatieafspraak met de juiste persoon wordt gemaakt. Het gebruik van het BSN is noodzakelijk voor de controle van de identiteit. BSN is daarnaast belangrijk, zodat in CoronIT automatisch de juiste persoonsgegevens geregistreerd worden in plaats van dat alle persoonsgegevens handmatig ingevoerd moeten worden (met het risico op administratieve fouten). Daarnaast is het BSN gekoppeld aan DigiD, wat het mogelijk maakt om de uitslag online in te zien. Het woonadres is nodig, zodat we de uitslag ook per brief kunnen toesturen

indien er onverhoopt een verkeerd telefoonnummer is geregistreerd en daardoor iemand de uitslag niet heeft kunnen ontvangen, of zijn/haar telefoon niet opneemt. De GGD is op basis van de Wet op de Geneeskundige Behandelovereenkomst (WGBO) ook verplicht om bepaalde gegevens vast te leggen. Dit is onder andere welke COVID-19 klachten de persoon in kwestie heeft, waar iemand is geweest en met wie hij/zij in contact is geweest. Ook wordt informatie vastgelegd van bron(nen) en nauwe contacten.

269. Wat voor screening en instructies hebben de medewerkers gekregen die met de coronasystemen werken?
De GGD heeft mij gemeld dat mensen een Verklaring Omtrent het Gedrag (VOG) moeten aanleveren en een geheimhoudingsverklaring ondertekenen. Dit is van toepassing op medewerkers van de GGD'en en van externe partijen. De training van de landelijke partners is hetzelfde, per GGD kan echter de training verschillen. De training is voor de start van werkzaamheden en periodiek. Verder is er bij de BCO-schil een systeem van feedback. Op basis daarvan wordt o.a. aanvullend opleidingsaanbod ontwikkeld (nspoh).

270. Klopt het dat IT-ers van de GGD GHOR niet vrijuit mogen spreken over de ICT-problemen? Zo ja, waarom niet?
De GGD heeft mij gemeld dat de GGD'en geen medewerkers onder druk hebben gezet om geen openheid van zaken te geven. In algemene zin wordt van medewerkers gevraagd om contacten met journalisten via de daarvoor beschikbare communicatiemedewerkers te laten lopen.

271. De leden van de PVV-fractie vragen de Minister ook hoe het nu zit met andere systemen bij de GGD? Is het systeem waarin vaccinaties worden bijgehouden wel veilig?
De GGD heeft mij gemeld dat gegevens van zowel testen en vaccineren zich bevinden in CoronIT, maar dat. het niet zo is dat alle medewerkers bij alle gegevens in CoronIT kunnen. Door middel van rollen en hieraan gekoppelde rechten wordt toegang verschaft. Iemand die vaccinatieafspraken maakt, kan wel de testgegevens zien omdat dat nodig kan zijn om te bepalen of een persoon gevaccineerd kan worden. Iemand die een testafspraak maakt, kan een vaccinatieafspraak wel zien, maar niet de overige bijbehorende medische gegevens. Ik heb aan GGD-GHOR gevraagd nog eens zeer kritisch tegen het licht te houden wat echt nodig is ten aanzien van deze functionaliteit voor het uitvoeren van testen en vaccineren en mij hierover op korte termijn te berichten. Overigens bevatte CoronIT tot voor kort een printfunctie die gebruikt werd bij noodprocedures. Deze functie is uitgezet.

272. Klopt het dat bij vaccinaties nog veel meer gegevens worden verzameld, zoals paspoortnummer en medische gegevens over bijvoorbeeld zwangerschap en/of allergieën?
De GGD heeft mij gemeld dat CoronIT de persoonsgegevens bevat die vereist zijn voor een medisch dossier (zie eerder antwoord), gegevens over de afspraak (tijd en plaats) en medische gegevens om te vaccinatie zorgvuldig toe te kunnen dienen rekening houdend met eventuele medische voorgeschiedenis (o.a. flauwvallen, allergische reacties, zwangerschap, gebruik van bloedverdunners). De uitvoeringsrichtlijn COVID-19 vaccinatie van het RIVM wordt gevolgd om te bepalen welke gegevens worden verzameld.

273. Wie heeft hiertoe, wanneer en op basis waarvan besloten?
De GGD heeft mij gemeld dat zij hebben besloten om CoronIT te gebruiken voor het registreren bij vaccinatie. Het besluit is genomen

nadat het Ministerie van VWS de GGD in december verzocht op korte termijn te starten met het grootschalig vaccineren in januari.

274. Is de voorzitter van de koepelvereniging GGD GHOR hiervan op de hoogte gebracht? Zo ja, wanneer? Zo nee, waarom niet?
De GGD heeft mij gemeld dat de voorzitter is geïnformeerd over het gebruik van CoronIT voor vaccinatie en over de daarvoor benodigde gegevens.

275. Is de Minister hier zelf van op de hoogte gebracht? Zo ja, wanneer? Zo nee, waarom niet?
276. Zijn ambtenaren op het Ministerie van VWS hiervan op de hoogte gebracht? Zo ja, wanneer? Zo nee, waarom niet?
Zowel de ambtelijk VWS als de Minister zijn er vanaf het begin bekend mee geweest dat CoronIT gebruikt zou gaan worden voor het vaccineren

277. De leden van de PVV-fractie vragen de Minister waarom de GGD denkt een paspoortnummer nodig te hebben voor de vaccinatie.
De GGD heeft mij gemeld dat vaccineren een geneeskundige handeling is. In de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) wordt onder de definitie van zorg zelfs expliciet verwezen naar art. 6b van de Wpg, namelijk het rijksvaccinatieprogramma waar COVID-19 onder valt. De GGD is in die zin een zorgverlener. Zorgverleners moeten een BSN registreren. Bij vaccinatie moeten mensen zich kunnen identificeren.

278. Waar wordt geregistreerd welk vaccin een gevaccineerde burger heeft gekregen? In het elektronisch patiëntendossier (EPD)? In het elektronisch medisch dossier (EMD)?
De GGD heeft mij gemeld dat CoronIT ten aanzien van vaccinaties een medisch dossier is. Het is een elektronisch dossier en daarmee kan het worden gezien als een EMD/EPD. CoronIT is een zorginformatiesysteem en geen elektronisch uitwisselingssysteem, omdat het niet gebruikt wordt om dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar te kunnen maken. Als de gevaccineerde instemt met uitwisseling van vaccinatiegegevens naar het RIVM, worden de gegevens daar bewaard o.a. met het oog op kunnen informeren bij eventuele bijwerkening. Idem als gevaccineerd instemt met uitwisseling naar de eigen huisarts.

279. Wat is het geval wanneer gevaccineerde burgers geregistreerd staan dat ze geen toestemming geven voor delen van hun EPD?
De GGD heeft mij gemeld da, in aansluiting op het antwoord op de vorige vraag CoronIT niet gedeeld wordt met anderen.

280. Hoe is die toestemming van gevaccineerde geregeld?
De GGD heeft mij gemeld dat dit wordt geregeld door het vragen van mondelinge toestemming bij het callcenters, die vervolgens wordt vastgelegd in CoronIT volgens protocol. Hierop vinden kwaliteitscontroles plaats.

281. Wat is de hoognodige informatie die de Minister nodig heeft voor een veilige privacy van gevaccineerde en waarom?
Ik begrijp de vraag zo dat dit over de centrale vaccinatie registratie bij het RIVM gaat. Bij reguliere vaccinatieregistraties bestaan twee afzonderlijke processen. Ten eerste de decentrale registratie bij de vaccineerders zoals de GGD'n. Dit betreft het medische dossier op grond van de WGBO en gaat over de zorgverlening. De tweede betreft een registratie bij het RIVM, die andere doelen dient. De registratie bij het RIVM heeft onder meer tot doel om bij te houden hoeveel mensen gevaccineerd zijn (vaccinatie-

graad), maar ook snel te kunnen handelen bij onverwachte situaties(bijvoorbeeld het uitvoeren van een recall), de veiligheid te bewaken en te meten hoe goed vaccins werken. Ik kan de leden van de PVV-fractie melden dat bij deze registratie de privacy wet -en regelgeving gevolgd wordt en dat privacy hoog in het vaandel staat. Ik draag via het RIVM op grond van de Wet publieke gezondheid zorg voor regie op de vaccinatie. Het RIVM heeft tot taak om de vaccinatie uit te voeren, te registreren, te bewaken en te beoordelen. Om dit te kunnen doen, registreert het RIVM de minimaal noodzakelijke persoonsgegevens over de vaccinatie in het registratiesysteem. Het RIVM administreert deze gegevens, nadat de betrokkene daarvoor (uitdrukkelijke) toestemming heeft gegeven aan de vaccineerder. De vaccineerder verstrekt deze gegevens vanuit haar decentrale registratie aan het RIVM. Het systeem waarin het RIVM registreert is het COVID-vaccinatie Informatie- en Monitoringsysteem (CIMS).

282. De leden van de PVV-fractie verwachten tot slot dat de coronasystemen inmiddels vervangen zijn door een systeem waarin de gegevens van burgers wel veilig zijn, zonder slag om de arm te houden. Genoemde leden ontvangen hier graag een toezegging op.
GGD GHOR Nederland laat op dit moment forensisch onderzoek uitvoeren naar de logging (de handelingen die in de GGD-systemen verricht zijn). En tot de start van automatisch en continu monitoren (naar verwachting eind maart gereed), blijven gespecialiseerde interne en externe teams voor de GGD'en de loggings controleren.

Vragen en opmerkingen van de CDA-fractie

De leden van de CDA-fractie maken van de gelegenheid gebruik om aanvullend aan de eerder gestelde schriftelijke vragen nog enkele vragen toe te voegen.
De leden van de CDA-fractie begrijpen dat de GGD snel wil stoppen met het programma HPZone voor bron- en contactonderzoek. Deze leden vragen de Minister op welke termijn er wordt overgestapt naar een ander portaal.

283. Wanneer is de GGD begonnen met het opzetten van het nieuwe portaal? Of wordt volgens de Minister hier gekozen voor een al bestaand beschikbaar alternatief, zoals Go.Data van de Wereldgezondheidsorganisatie?
GGD GHOR Nederland heeft mij laten weten dat zij voorhet bron- en contactonderzoek overgaan naar een nieuwe voorziening. Dat zal versneld gaan gebeuren. Het exacte moment is nog niet bekend; de activiteiten zijn gericht op een overgang in maart. De noodzakelijke functionaliteit voor COVID-19-bestrijding dient aanwezig te zijn.

284. Op welke wijze wordt geborgd dat het nieuwe portaal wél veilig zal zijn en geschikt is voor het grootschalige bron- en contactonderzoek?
De GGD heeft mij gemeld dat zij continu bezig zijn om onze werkprocessen te verbeteren en de veiligheid van onze systemen te vergroten. Welke maatregelen precies genomen worden zullen, omwille van de veiligheid, niet toegelicht worden.

285. Welke verdere maatregelen worden genomen met betrekking tot het systeem dat testinformatie vastlegt?
De GGD heeft mij gemeld dat, tot de lancering van volautomatisch en continu controleren eind maart, zij gespecialiseerde interne en externe teams voor de GGD'en de loggings blijven controleren.

286. Wat betekenen de datalekken voor de aanpak omtrent vaccinregistratie, mede gezien het feit dat apothekers hebben aangeboden hun bestaande systeem daarvoor te gebruiken?
Ik kan de leden van de CDA-fractie melden dat het aan iedereen die vaccineert, zoals GGD'en, is om zelf de systemen te kiezen die ze voor hun registratie gebruiken. Daarbij moeten zij onder meer zorgen voor de nodige technische en organisatorische maatregelen om het systeem afdoende te beveiligen. Dat geldt ook voor de registratie van de vaccinaties.
De leden van de CDA-fractie begrijpen uit de media dat inmiddels tientallen medewerkers van de GGD ontslagen zijn vanwege ongeoorloofd gebruik van de systemen.

287. Genoemde leden vragen de Minister of deze medewerkers alleen ontslagen zijn, of dat ook verdere acties richting hen is ondernomen. Welke acties zijn naar aanleiding van deze ontslagen ondernomen om dergelijk ongeoorloofd gebruik in het vervolg te voorkomen?
De GGD heeft mij gemeld dat circa 30 keer medewerkers zijn ontslagen. Het is niet bekend of er verdere acties tegen hen zijn ondernomen.

288. Wat is er met de signalen gedaan van eigen medewerkers die maanden geleden al waarschuwden dat hun systemen kwetsbaar waren voor datadiefstal? Hoe komt het dat met die signalen niets is gedaan?
De GGD heeft mij gemeld dat er één signaal formeel is binnen gekomen bij GGD GHOR Nederland van medewerkers, hierop is gereageerd en geacteerd. Op dit moment is er geen totaaloverzicht van klachten of meldingen door medewerkers die ingediend zijn bij GGD'en en de opvolging daarvan.
Het bron- en contactonderzoek wordt door de GGD in opdracht van het Ministerie van VWS uitgevoerd.

289. De leden van de CDA-fractie vragen de Minister of het klopt dat het Ministerie van VWS daarmee formeel ook opdrachtgever is voor de ICT-systemen die hiervoor gebruikt worden? Zo ja, welke opdracht heeft het Ministerie van VWS de GGD gegeven omtrent de ontwikkeling van het systeem?
Nee, de GGD'en zijn zelf opdrachtgever voor het ICT-systeem ter ondersteuning van het bron- en contactonderzoek. Momenteel wordt in opdracht van de GGD een nieuw systeem ontwikkeld ter vervanging, GGD Contact.

290. Is gecontroleerd of aan de voorwaarden van de opdracht is voldaan? Zo ja, hoe? Zo nee, waarom niet?
Zie het antwoord op vraag 289.

291. De leden van de CDA-fractie vragen de Minister welke mogelijkheden er zijn een nieuw BSN te krijgen voor mensen die te horen krijgen dat hun gegevens gelekt zijn. Worden mensen hier actief op gewezen?
Op dit moment is het op grond van de Wet algemene bepalingen burgerservicenummer (artikel 8) niet mogelijk een BSN te wijzigen. Dit kan alleen indien een BSN foutief is toegekend, waarvan in het geval van een vermoeden van verhoogd risico op misbruik na een datalek geen sprake is. Het is ook niet nodig om een nieuw BSN aan te maken. Zoals hierboven aangaf bij de beantwoording van de vragen van SGP-fractie is de kans op fraude met alleen het BSN klein. Ook met een BSN in combinatie met naam, adres en woonplaats kunnen geen bankrekeningen worden geopend of telefoonabonnementen worden afgesloten.
Wanneer er daadwerkelijk misbruik is gemaakt van gelekte persoonsgegevens wordt de burger doorverwezen naar het Centraal Meldpunt

Identiteitsfraude en -fouten bij de Rijksdienst voor Identiteitsgegevens en kan er aangifte bij de politie worden gedaan.

Vragen en opmerkingen van de D66-fractie

De leden van de D66-fractie hebben een groot aantal vragen gesteld in het schriftelijk overleg op 28 januari jl. over illegale handel in data afkomstig uit GGD-systemen. Deze vragen en opmerkingen gingen onder andere over de opbouw van de datasets, de bronnen voor de datasets, de toegang tot de datasets, de beveiliging van de systemen, de risico's voor burgers en overige zaken. Genoemde leden kijken uit naar de beantwoording van de Minister voorafgaand aan het debat met de Minister van VWS en de Minister voor Rechtsbescherming over de illegale handel in data afkomstig uit GGD-systemen. Dit debat is aangevraagd door de leden van de D66-fractie, met steun van de SP, PvdA, Denk, PVV, 50PLUS, PvdD, SGP, GroenLinks en het lid Van Kooten Arissen. Genoemde leden zijn echter geschokt na nieuwe onthullingen over de omvang van het datalek bij de GGD en hebben daarom nog aanvullende vragen aan de Minister.

292. Genoemde leden horen graag van de Minister wanneer de eerste signalen over kwetsbaarheden binnen de GGD-systemen en ongeoorloofd gebruik van de systemen terecht zijn gekomen bij de voorzitter van de GGD GHOR en bij de Minister zelf.
Voor antwoord op deze vraag verwijs ik u naar vraag 260.

293. Wat is gebeurd met de signalen die meerdere GGD-medewerkers zeggen te hebben gegeven over de kwetsbaarheden van de GGD-systemen? Wanneer is op basis van deze signalen voor het eerst actie ondernomen?

293. Kan de Minister een uitputtende lijst geven wie op de hoogte was van deze signalen (op het Ministerie van VWS)?
294. Hoe vaak is de Minister over deze signalen geïnformeerd?
295. Hoe lang waren de signalen op ambtelijk niveau bekend, voordat de Minister hierover is geïnformeerd?
296. Op welke dag is de Minister over de signalen geïnformeerd en op welk moment heeft de Minister in dit kader stappen ondernomen?
297. Kan de Minister de Kamer alle onderliggende stukken waarin deze signalen aan de orde komen toesturen?
298. Genoemde leden vragen de Minister hoe het mogelijk is dat de GGD zegt niet bekend te zijn met waarschuwingen van eigen medewerkers.
Voor de antwoorden op de 293, 294, 295, 296,297 en 298 verwijs ik naar het antwoord op vraag 260.

299 Welke acties heeft de voorzitter van de GGD GHOR volgende de Minister ondernomen na de eerste signalen over kwetsbaarheden binnen de GGD-systemen en ongeoorloofd gebruik van de systemen?
De GGD heeft mij gemeld dat het niet bekend is of de vorige voorzitter is geïnformeerd. Eind oktober is de huidige voorzitter op hoofdlijnen geïnformeerd over zwakheden in systeem (continuïteit, betrouwbaarheid en veiligheid) en het ingezette verbeterplan.

300. De leden van de D66-fractie horen graag van de Minister hoe het mogelijk is dat de verplichte risicoanalyse van gegevensverwerking systemen pas een half jaar na introductie van de systemen af was.
De GGD heeft mij gemeld dat voor CoronIT vanaf het begin en tijdens de ontwikkeling van het systeem een continue risicoanalyse is uitgevoerd, zowel voor testen, het callcenter en vaccineren. Omdat de processen constant onderhevig zijn aan (ad hoc) veranderingen, wordt de risicoanalyse constant bijgehouden en gewijzigd. Het is met andere woorden,

een levend document. Daaruit zijn risico's naar boven gekomen, die door de GGD GHOR Nederland of wel zijn gemitigeerd, opgelost, of op basis van een afweging zijn geaccepteerd.

301. Wat was de reactie van de Autoriteit Persoonsgegevens (AP) op de risicoanalyse?
De GGD heeft mij gemeld dat de Autoriteit Persoonsgegevens op de door haar ontvangen informatie en risicoanalyse geen verdere vragen heeft gesteld.

302. Welke acties zijn op basis van deze reactie ondernomen? Kan de Minister per actie aangeven wanneer deze precies zijn ondernomen?
De GGD heeft mij gemeld dat de Autoriteit Persoonsgegevens op de door haar ontvangen risicoanalyse geen verdere vragen heeft gesteld.

303. Kan de Minister bevestigen dat ook securitybedrijf FOX-IT CoronIT heeft doorgelicht? Welke resultaten kwamen uit deze doorlichting en wat is wanneer met de resultaten gedaan?
De GGD heeft mij gemeld dat risicoanalyses vertrouwelijke informatie bevatten en kunnen om veiligheidsredenen niet worden gedeeld met de Kamer.

304. Heeft de Minister waarschuwingen ontvangen van de Begeleidingscommissie Digitale Ondersteuning Bestrijding COVID-19 over de kwetsbaarheid van de systemen? Wat is er met de waarschuwing gedaan?
Het antwoord daarop is dat de Begeleidingscommissie Digitale Ondersteuning Bestrijding Covid-19 hun zorgen over de kwetsbaarheid van de systemen direct en alleen met GGD GHOR Nederland heeft gedeeld en besproken. Ik ben daar niet van op de hoogte gesteld.

305. Was de Minister op de hoogte van de zorgen van de Autoriteit Persoonsgegevens (AP), FOX-IT en de begeleidingscommissie? Zo ja, wanneer en hoe? Kan de Minister hiervan onderliggende stukken delen?
Voorzover ik heb kunnen nagaan ben ik hiervan niet op de hoogte gesteld.
De leden van de D66-fractie zijn verontrust dat volgens de Fraudehelpdesk vorig jaar al sprake was van oplichting met behulp van gegevens van burgers die gestolen werden bij de GGD.

306. Is er contact geweest tussen de Fraudehelpdesk en de GGD en/of het Ministerie van VWS? Zo ja, wanneer?
307. Welke acties zijn ondernomen na het contact met de Fraudehelpdesk?
De Fraudehelpdesk geeft aan dat dit niet het geval is geweest.

308. Zijn ook via andere kanalen signalen binnengekomen over mogelijke fraude met gegevens afkomstig uit GGD-systemen? Zo ja, wanneer en hoeveel?
De Fraudehelpdesk geeft aan dat er zo'n 40 meldingen zijn ontvangen die betrekking hadden op verdachte telefoontjes namens de GGD. De AP heeft de laatste week bijna 100 telefoontjes ontvangen van verontruste burgers over de problemen bij de GGD. Ook zijn in die week circa 90 klachten ontvangen van burgers met betrekking tot de verwerking van (hun) persoonsgegevens door de GGD.

309. Wat is de geschatte omvang van de datahandel en het aantal aanbieders van illegaal verkregen data?
De GGD heeft mij gemeld dat op dit moment onduidelijk is wat de omvang is van het aantal data dat gestolen is. Dat is onderdeel van het politieonderzoek.

310. Wat gaat de Minister doen voor de slachtoffers van de datahandel?

Ik kan hen melden dat ik eerst het onderzoek van de politie afwacht, zodat we weten om hoe veel mensen het precies gaat. Vervolgens kunnen we gaan kijken naar een passende oplossing voor de slachtoffers van de datahandel.

311. Hoeveel medewerkers zijn volgens de Minister exact ontslagen bij de GGD vanwege ongeoorloofd gebruik van de systemen?
Op basis van steekproeven is circa 30 keer een medewerker ontslagen.

312. Wanneer vonden de eerste ontslagen plaats?
De GGD heeft mij gemeld dat het exacte moment van de eerste ontslagen niet bekend is. In totaal zijn de afgelopen periode circa 30 medewerkers ontslagen.

313. Wanneer waren deze ontslagen bekend bij de Minister? Het behoort tot de verantwoordelijkheid van de werkgever zelf om dergelijke kwesties af te handelen.
Ik ben niet geïnformeerd over ontslagen bij de GGD GHOR. De GGD heeft mij gemeld dat de ontslagen het gevolg waren van steekproefsgewijze controles op de loggings. Er is één signaal formeel binnen gekomen bij GGD GHOR Nederland van medewerkers, hierop is gereageerd en geacteerd. Op dit moment is er geen totaaloverzicht van klachten of meldingen door medewerkers die ingediend zijn bij GGD'en en de opvolging daarvan.

314. Als er medewerkers van de GGD ontslagen zijn vanwege ongeoorloofd gebruik van de systemen, hoe is het volgens de Minister dan mogelijk dat de GGD zegt niet bekend te zijn met signalen van kwetsbaarheden vanuit medewerkers?
Voor het antwoord op deze vraag verwijs ik u naar vraag 313.

315. De leden van de D66-fractie horen graag van de Minister of de voorzitter van de GGD GHOR en de Minister zijn ingelicht over tekortkomingen van het waarborgen van de privacy in GGD-systemen om te voldoen aan de eisen uit de Europese Algemene verordening gegevensbescherming (AVG)? Zo ja, wanneer zijn zij hierover ingelicht?
Beiden zijn op hoofdlijnen geïnformeerd over de kenmerken van de IT-ondersteuning waarmee gewerkt werd ten behoeve van de uitvoering van het testen, traceren en vaccineren. Verder verwijs ik naar de risicoanalyse waarover de Kamer in de brief van 24 december jl. is geïnformeerd.

316. Kan de Minister aangeven welke actie vervolgens zijn ondernomen door de voorzitter van de GGD GHOR en de Minister zelf?
De risicoanalyses zijn intern binnen GGD GHOR Nederland besproken. Daarnaast is een werkgroep aan de slag gegaan met opvolging van de uitgevoerde risico inventarisatie onder de Regiegroep DOTT. Een werkgroep follow-up risico inventarisatie draagt zorg voor een verbeterplan, dat ik deze week verwacht te ontvangen.

317. Genoemde leden horen graag via welke stappen de Minister van plan is te zorgen dat de GGD-systemen voldoen aan de privacy waarborgen en de richtlijnen van de AVG. Op welke termijn is dit volgens de Minister gewaarborgd?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

318. Welke maatregelen worden in de tussentijd genomen om gegevens van burgers zo goed mogelijk te beschermen bij de GGD, zodat zij zich zonder zorgen kunnen laten testen?

De GGD heeft mij gemeld dat sinds de zomer van 2020 diverse maatregelen zijn getroffen om het toegangsbeheer te verscherpen en om controles uit te voeren op de toegang tot en het gebruik van persoonsgegevens. Gedurende de gehele periode zijn autorisaties verscherpt, waarbij bij CoronIT in eerste instantie aandacht is uitgegaan naar de scheiding van rollen en inrichting van de rollen, vervolgens naar de logging van activiteiten en is een project gestart om geautomatiseerde controle hierop plaats te laten vinden.
Voor HPZone (Lite) zijn extra logging functionaliteiten ingericht, is een risicoanalyse uitgevoerd om verdere risico's te identificeren, zijn de aanbevelingen opgepakt en vertaald in een aantal maatregelen, is een project gestart om toegang beter te loggen en monitoren. Verder verwijs ik naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

319. Hoe staat het met de informatiebeveiliging van de systemen die wordt gebruikt bij het vaccineren?
Zie hiervoor het antwoord op vraag 177.

320. Worden in deze systemen meer persoonsgegevens vastgelegd in vergelijking met het proces omtrent testen? Om welke gegevens gaat het?
De GGD heeft mij gemeld dat in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) onder de definitie van zorg zelfs expliciet wordt verwezen naar art. 6b van de Wpg, namelijk het rijksvaccinatieprogramma waar COVID-19 onder valt. In CoronIT, het systeem voor testen en vaccineren, staan onder andere naam, adres, woonplaats, telefoonnummer/e-mailadres, BSN, geslacht, geboortedatum, test- en/of vaccineerafspraken en testresultaten. Contra-indicaties en COVID-19 klachten.
De gegevens zoals geregistreerd in CoronIT zijn opgenomen in de privacyverklaring CoronIT. Het BSN is noodzakelijk voor de controle van de identiteit. BSN is daarnaast belangrijk, zodat in CoronIT automatisch de juiste persoonsgegevens geregistreerd worden in plaats van dat alle persoonsgegevens handmatig ingevoerd moeten worden (met het risico op administratieve fouten). Daarnaast is het BSN gekoppeld aan DigiD, wat het mogelijk maakt om de uitslag online in te zien. Het woonadres is nodig, zodat de GGD'en de uitslag ook per brief kunnen toesturen indien er onverhoopt een verkeerd telefoonnummer is geregistreerd en daardoor iemand de uitslag niet heeft kunnen ontvangen.

321. De leden van de D66-fractie hebben vernomen dat door externe private organisaties, zoals Teleperformance, veelvuldig WhatsApp werd gebruikt voor het delen van (bijzondere) persoonsgegevens van burgers. Hoe is het volgens de Minister mogelijk dat Teleperformance stelt dat het hier «persoonlijke keuzes van medewerkers om met collega's een app-groep aan te maken» betreft?
De GGD heeft mij gemeld dat de informatie vooral werd gedeeld vanuit functioneel oogpunt: om collega's snel vooruit te helpen met hun werkzaamheden. Het beleid van de GGD'en is dat het uitwisselen van privacygevoelige informatie via Whatsapp niet toegestaan is. Rocketchat is een communicatieplatform dat werd gebruikt voor interne communicatie en communicatie tussen callcenteragents onderling bij het call center om afspraken te maken voor de teststraat (Teleperformance). Rocketchat liep inderdaad zo nu en dan vast. Medewerkers hebben inderdaad Whatsappgroepen gemaakt. Dit is door Teleperformance echter altijd ontmoedigd. Rocketchat is inmiddels vervangen door Blackboard.

322. Is hiervan ook sprake van bij andere externe private organisaties?
Voor het antwoord op deze vraag verwijs ik naar vraag 321.

323. Was dit bekend bij het Ministerie van VWS? Zo ja, wanneer?

Het ministerie is hiervan niet op de hoogte gesteld.

324. Is er volgens de Minister actie ondernomen tegen het gebruik van ongeschikte systemen voor het delen van gevoelige privégegevens?
De GGD heeft mij gemeld dat Rocketchat inmiddels is vervangen door Blackboard.

Vragen en opmerkingen van de GroenLinks-fractie

De leden van de GroenLinks-fractie hebben met verbazing kennisgenomen van het bericht dat de GGD al maandenlang op de hoogte was van de ernstige problemen rond de bescherming van persoonsgegevens in de digitale coronasystemen, en dat die problemen desondanks konden voortduren. Deze leden hebben daar nog veel vragen over.

325. Allereerst willen de leden van de GroenLinks-fractie graag weten hoe de Minister reageert op de berichtgeving van RTL Nieuws dat de GGD al maanden op de hoogte was van de problemen en dat interne kritiek van medewerkers en leidinggevenden steeds werd weggewuifd? Hoe is het dan mogelijk dat de GGD stelt niet bekend te zijn met deze signalen?
Ik verwijs u naar de brief die aan uw Kamer is verzonden op 2 februari jl.

326. Was het Ministerie van VWS volgens de Minister bekend met deze signalen dat interne kritiek werd weggewuifd? Zo ja, wanneer en wat is daarmee gedaan?
Voor het antwoord op deze vraag verwijs ik naar vraag 260.

327. Genoemde leden vragen de Minister tevens of de berichtgeving in de Volkskrant klopt dat de algemene zorgen bij het Ministerie van VWS over de veiligheid van persoonsgegevens in de coronasystemen al sinds het voorjaar van 2020 bestaan?[3] Zo ja, welke signalen waren de aanleiding voor die zorgen, op welke wijze kwamen die signalen binnen bij het ministerie, en wat is er destijds met die signalen en zorgen gedaan?
Ik weet niet waar deze berichtgeving op is gebaseerd. In mijn brief van 19 mei aan uw Kamer (Kamerstuk 25 295, nr. 317) wordt gemeld dat de voorbereidingen van de IT applicatie CoronIT op schema lopen, en aangegeven dat hierbij voldaan wordt aan de eisen van veilig gebruik van burgers.

328. In dit kader vragen deze leden de Minister ook nogmaals toe te lichten op welke wijze de opdracht voor het ontwerp van de coronasystemen werd gegeven? Wanneer gaf het Ministerie van VWS welke opdracht aan de GGD op dit vlak, en in hoeverre was bij die opdracht specifiek aandacht voor privacy by design, bescherming van persoonsgegevens, doelbinding, dataminimalisatie en autorisatiebeheer gericht op het beperken van toegang tot persoonsgegevens tot het strikt noodzakelijke?
Begin april 2020 heb ik GGD GHOR de opdracht gegeven voor de (door)ontwikkeling van en aansluiting van verschillende GGD'en op CoronIT. De afspraken zijn vastgelegd in een dienstverleningsovereenkomst. Bij de ontwikkeling van CoronIT zijn de uitgangspunten van privacy by design en security leidend geweest.

---

[3] De Volkskrant, 28 januari 2021, «Datalek GGD betreft ook gevaccineerden, ministerie had al vanaf begin zorgen» (https://www.volkskrant.nl/nieuws-achtergrond/datalek-ggd-betreft-ook-gevaccineerden-ministerie-had-al-vanaf-begin-zorgen~b0c217ba/#:~:text=Nieuws-,Datalek%20GGD%20betreft%20ook%20gevaccineerden%2C%20ministerie%20had%20al%20vanaf%20begin,en%20gezondheidsverklaringen%20van%20gevaccineerde%20personen)

329. En in hoeverre heeft het Ministerie van VWS destijds bij de GGD aangedrongen op een gedegen Data Protection Impact Assessment? Klopt het dat deze pas veel later is uitgevoerd? Zo ja, wanneer? En waarom heeft het Ministerie van VWS daar volgens de Minister niet scherper op toegezien?
De verantwoordelijkheid voor het opstellen van een Data Protection Impact Assessment ligt bij de GGD'en en GGD GHOR. Vanuit mijn rol heb ik hier niet op aangedrongen.

330. Klopt de berichtgeving in de Volkskrant dat het ministerie in augustus hulp heeft aangeboden aan de GGD om de privacy problemen op te lossen, maar dat deze hulp categorisch werd geweigerd door de GGD? Zo ja, en als het Ministerie van VWS al in het voorjaar op de hoogte was van de problemen, waarom is het Ministerie van VWS zich er dan pas in augustus actief mee gaan bemoeien? En wat was de reactie van het Ministerie van VWS op de afhoudende respons van de GGD? Waarom heeft het Ministerie van VWS niet geëist dat de systemen zouden worden doorgelicht en aangepast?
Ik weet niet waar deze berichtgeving op is gebaseerd. In mijn brief van 19 mei aan uw Kamer (Kamerstuk 25 295, nr. 317) wordt gemeld dat de voorbereidingen van de IT applicatie CoronIT op schema lopen, en aangegeven dat hierbij voldaan wordt aan de eisen van veilig gebruik van burgers.

331. Kan de Minister verder heel specifiek aangeven wanneer en op welke wijze het Ministerie van VWS precies op de hoogte was van het bestaan van een exportfunctie in het systeem, toegankelijk voor duizenden medewerkers, waarmee gericht gegevens in het systeem kunnen worden opgezocht en gedownload naar vrij deelbare Excel of pdf-bestanden? Wat heeft het Ministerie van VWS op dat moment ondernomen?
VWS was niet tot op detailniveau op de hoogte van het systeem, totdat de exportfunctie onderdeel werd van de veiligheidsissues. Voor een overzicht van acties die ik heb ondernomen verwijs ik u naar de Kamerbrief hierover van 2 februari 2021.

332. De leden van de GroenLinks-fractie vragen de Minister ook in te gaan op de beschrijving, van RTL Nieuws, van de controles van medewerkers. Klopt het dat deze controle op enig moment bestond uit het periodiek (eens in de zoveel maanden) delen van het scherm en openen van de digitale prullenbak om te kijken of zich daar gestolen gegevens bevonden?
De GGD heeft mij gemeld dat de controles steekproefsgewijs plaatsvinden. De controles zien op logging (zoekopdrachten en toegang). GGD GHOR Nederland laat op dit moment forensisch onderzoek uitvoeren naar de logging (de handelingen die in de GGD-systemen verricht zijn). En tot de start van automatisch en continu monitoren, blijven gespecialiseerde externe teams voor de GGD'en de loggings controleren. Daarnaast heeft GGD GHOR Nederland een team dat 7 dagen per week handmatig verdachte handelingen opspoort.

333. Zo ja, wat vindt de Minister van een dergelijke manier van controleren? En hoe verhoudt deze wijze van controleren zich tot de uitspraken van de Minister tijdens de beantwoording van mondelinge vragen, waar hij zei dat de GGD al sinds het begin van de coronapandemie continu controleert op het gebruik van de systemen? Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

Genoemde leden zijn ook benieuwd naar hoe de GGD en het Ministerie van VWS hebben gereageerd op de berichtgeving in september door Nieuwsuur over privacy problemen bij de digitale systemen van de GGD.

334. Hoe kan het volgens de Minister dat die berichten niet alle alarmbellen hebben doen afgaan, bij zowel de GGD als het Ministerie van VWS?
Ik heb uw Kamer in antwoord op schriftelijke vragen van de leden Hijink (SP) (Aanhangsel Handelingen II 2020/21, nr. 825) en Ellemeet, Smeulders en Buitenweg (GroenLinks) (Aanhangsel Handelingen II 2020/21, nr. 826) hierover geïnformeerd, en daarbij aangegeven welke maatregelen de GGD GHOR al sinds de start van het traject heeft getroffen om de privacy en vertrouwelijkheid van persoonsgegevens te borgen.
Voor het antwoord op deze vraag verwijs ik u verder naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

335. Klopt het dat de GGD naar aanleiding van die berichten ook een officiële waarschuwing kreeg van de AP?
De GGD heeft mij gemeld dat de Autoriteit Persoonsgegevens geen officiële waarschuwing heeft gegeven naar aanleiding van de berichtgeving van Nieuwsuur.

336. Was het Ministerie van VWS daar ook van op de hoogte?
Zie antwoord op vraag 335.

337. Hoe kan het dat de problemen zelfs na die berichtgeving van Nieuwsuur en de waarschuwing van de AP nog steeds door konden gaan?
De GGD heeft mij gemeld dat de AP geen officiële waarschuwing heeft gegeven naar aanleiding van de berichtgeving van Nieuwsuur.
Bij aanvang van de ontwikkeling en het gebruik van CoronIT ging het over een substantieel kleinere gebruikersomvang. Gedurende de verdere opschaling van het test- en traceerbeleid is de robuustheid en schaalbaarheid van het systeem continu punt van aandacht geweest. Daarbij is een continue afweging gemaakt tussen aanpassingen om beleidswijzigingen te ondersteunen en aan gebruikersvriendelijkheid, bedrijfscontinuïteit en privacy.
Voor HPZone geldt dat individuele GGD'en een contract hebben met de leverancier en dit niet centraal in één hand ligt. Er is meermalen getracht deze situatie te veranderen en afspraken te maken met de leverancier. Het doorvoeren van maatregelen bleef gecompliceerd en daarom is besloten te starten met het ontwikkelen van een nieuw systeem en over te gaan zodra mogelijk.
In dit kader verzoeken de leden van de GroenLinks-fractie de Minister om alle communicatie tussen het Ministerie van VWS en de GGD over de privacy problemen van de digitale coronasystemen, sinds het begin van de coronapandemie, met de Kamer te delen.

338. Is de Minister bereid om dit te doen?
Ik heb u als bijlagen een aantal stukken gestuurd. Gegeven het korte tijdsbestek kan ik niet uitsluiten dat er aanvullende informatie beschikbaar zou zijn.

339. De leden van de GroenLinks-fractie horen ook graag van de Minister of de berichtgeving in de Volkskrant klopt dat testmedewerkers het dossier van gevaccineerde personen kunnen bekijken zonder dat daar noodzaak toe is. Zo ja, hoe verhoudt dat zich tot de beantwoording van de Minister op mondelinge vragen op 26 januari jl., waarin hij aangaf dat dit niet kan?
De GGD heeft mij gemeld dat de gegevens van zowel testen en vaccineren zich in CoronIT bevinden, maar. dat het niet zo is dat alle medewerkers bij alle gegevens in CoronIT kunnen. Door middel van rollen en hieraan gekoppelde rechten wordt toegang verschaft. Iemand die vaccinatieafspraken maakt, kan wel de testgegevens zien omdat dat nodig kan zijn om te bepalen of een persoon gevaccineerd kan worden. Iemand die een testafspraak maakt, kan een vaccinatieafspraak wel zien, maar niet de

overige bijbehorende medische gegevens. Ik heb aan GGD-GHOR gevraagd nog eens zeer kritisch tegen het licht te houden wat echt nodig is ten aanzien van deze functionaliteit voor het uitvoeren van testen en vaccineren en mij hierover op korte termijn te berichten. Overigens bevatte CoronIT tot voor kort een printfunctie die gebruikt werd bij noodprocedures. Deze functie is uitgezet.

340. Gezien het feit dat de GGD en het Ministerie van VWS al op de hoogte waren van privacy problemen rond CoronIT, vragen de leden van de GroenLinks-fractie verder waarom de Minister ervoor heeft gekozen om juist dit systeem breder in te zetten en ook te gebruiken voor vaccinaties? In hoeverre hebben de zorgen over de privacy bij CoronIT een rol gespeeld bij deze beslissing?
De GGD heeft mij gemeld dat door de genomen extra maatregelen er geen reden is om aan te nemen dat het CoronIT systeem onveilig is. De genomen maatregelen zien toe op het beperken van recht en het controleren van gedrag. Beide betreffen dus het gebruik van het systeem. Gezien de korte tijd die beschikbaar was tussen het moment dat de Minister de GGD vroeg om de vangnetfunctie in te vullen met het grootschalig vaccineren en het moment dat gestart moest worden was het daarom niet wenselijk en niet nodig om uit te wijken naar een ander systeem. Als die keuze wel was gemaakt was het ook niet mogelijk geweest om begin januari de vaccinatiecampagne te starten.

341. Waarom is er, op basis van die kennis van bestaande problemen, niet voor gekozen een ander systeem te gebruiken of een nieuw systeem voor te ontwikkelen?
De GGD heeft mij gemeld dat uit wijken naar een ander systeem een langere ontwikkel- en trainingstijd gevergd zou hebben waardoor starten met (afspraken maken voor) vaccineren ernstig in het gedrang zou komen. GGD GHOR Nederland had, gezien de gewenste tijdlijnen, geen andere keuze dan het gebruiken van het bestaande systeem. De signalen van de GGD'en wezen niet op problemen met privacybescherming of informatiebeveiliging op dat moment.

342. zijn er toen aanvullende eisen gesteld, gegeven de keuze voor CoronIT en de bestaande zorgen daarover? Zo nee, waarom niet?
De GGD heeft mij gemeld dat er aanvullende eisen zijn gesteld aan de leverancier op het gebied van capaciteit van de applicatie en het team dat de applicatie ondersteunt. Daarnaast is een aparte DPIA uitgevoerd en zijn speciale autorisatierollen voor vaccineren ontworpen en geïmplementeerd, zodat medische gegevens naar behoren zijn afgeschermd.
De leden van de GroenLinks-fractie zijn benieuwd hoe de Minister nu, met de wetenschap van het grootschalige datalek, terugkijkt op alle beslissingen die zijn genomen rond de digitale systemen ter ondersteuning van het testen, bron- en contactonderzoek en vaccineren.

343. In hoeverre heeft haast een rol gespeeld bij de onzorgvuldigheid met betrekking tot de privacy? Welke andere factoren dan haast ziet de Minister en welke lessen trekt hij hieruit?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.
344. En welke verantwoordelijkheid vindt de Minister dat het Ministerie van VWS als opdrachtgever draagt voor schade die slachtoffers van het datalek ondervinden, gezien de verschillende besluiten die zijn genomen?
Ik verwijs u graag naar het antwoord op vraag 3.

345. Tenslotte horen de leden van de GroenLinks fractie graag of het klopt dat de GGD heeft aangegeven zo snel mogelijk af te willen van het systeem HPZone voor bron- en contactonderzoek en met man en macht

werkt aan een ander, veiliger portaal. Zo ja, kan de Minister aangeven welke partijen de GGD daarbij heeft betrokken en op welke termijn men de overstap kan maken? Geldt dit ook voor het CoronIT systeem? Zo nee, waarom niet?
GGD GHOR Nederland heeft mij gemeld dat zij voor het bron- en contactonderzoek overgaan naar een nieuwe voorziening. Dat zal versneld gaan gebeuren. Het exacte moment is nog niet bekend; de activiteiten zijn gericht op een overgang in maart. De noodzakelijke functionaliteit voor COVID-19-bestrijding dient aanwezig te zijn.

Vragen en opmerkingen van de SP-fractie

De leden van de SP-fractie vinden het zorgwekkend dat niet geluisterd is naar medewerkers van de GGD die meermaals melding hebben gemaakt van de privacy problemen. Genoemde leden vragen hoe het mogelijk is dat niets met deze signalen is gedaan? Kan de Minister aangeven op welke gronden de GGD hulp weigerde van het Ministerie van VWS bij bijvoorbeeld het verbeteren van het systeem?

346. Voorts vragen deze leden de Minister wat de rol van de AP in deze kwestie is. In hoeverre en sinds wanneer was de AP op de hoogte van de kwetsbaarheden van het systeem van de GGD?
De AP houdt in de breedste zin toezicht op de juiste verwerking van de persoonsgegevens. Mij is bekend dat de GGD'en recentelijk een melding hebben gedaan van kwetsbaarheden. Over deze meldingen informeert de AP mij niet.

347. Hoe is het mogelijk dat er geen risicoanalyse is uitgevoerd?
De GGD heeft mij gemeld dat op basis van een risicoanalyse al extra maatregelen gepland waren. Na de risicoanalyse is een gespecialiseerde externe partij ingeschakeld om het project voor inrichting van geautomatiseerde monitoring te versnellen en extra specialistische kennis toe te voegen om de inrichting van deze monitoring verder vorm te geven.

348. Ook vragen deze leden de Minister hoe het mogelijk is dat berichtgeving in de media verscheen dat de AP de GGD onder verscherpt toezicht heeft gesteld, terwijl later is gebleken dat de AP niet over een dergelijk instrument beschikt en de GGD ook niet op de hoogte was van deze stap.
349. Kan de Minister aangeven welke handhaving de AP wel toepast?
De AP verscherpt het toezicht vanwege de ernst van de zaak. Met deze vorm van toezicht wil de AP monitoren of en zo mogelijk vaststellen dat de GGD toereikende maatregelen neemt gericht op de beveiliging van gevoelige gegevens. Dat betekent dat inspecteurs van de AP de ontwikkelingen bij de GGD nauwlettend volgen. Zij gaan na te of noodzakelijke verbeteringen in de beveiliging worden uitgevoerd, en of de uitvoering in lijn is met de plannen. Er worden door de AP ook controles uitgevoerd om vast te stellen of de persoonsgegevens goed worden beveiligd. Verder vraagt de AP om periodieke evaluaties van de GGD. De term verscherpt toezicht heeft betrekking op de vorm en de intensiteit van het toezicht door een toezichthouder of inspectie. Het is aan de AP vast te stellen welke vorm van toezicht noodzakelijk is.

350. De leden van de SP-fractie vragen de Minister hoeveel meldingen van (vermoedelijke) fraude naar aanleiding van het datalek bij de GGD inmiddels zijn binnengekomen bij het Fraudehelpdesk en wat de aard is van deze meldingen.
De Fraudehelpdesk geeft aan dat het in totaal zo'n 40 meldingen heeft ontvangen die betrekking hadden op verdachte telefoontjes namens de

GGD. Een tiental ervan is door de Fraudehelpdesk aangemerkt als (vermoedelijk) frauduleus.

351. De leden van de SP-fractie hebben begrepen dat inmiddels besloten is te stoppen met HPZone, het systeem dat in gebruik was en niet geschikt is voor de hoeveelheid bron- en contactonderzoeken per dag. Genoemde leden vragen de Minister welk systeem het meest geschikt is voor het uitvoeren van het bron- en contactonderzoek en hoe gewaarborgd wordt dat in de toekomst dergelijke problemen worden voorkomen.
GGD GHOR Nederland heeft mij gemeld dat zij overgaan naar een nieuwe voorziening. Dat zal versneld gaan gebeuren. Het exacte moment is nog niet bekend; de activiteiten zijn gericht op een overgang in maart. De noodzakelijke functionaliteit voor COVID-19-bestrijding dient aanwezig te zijn.

352. Wat is de reden om wel te stoppen met HPZone, maar niet met CoronIT, terwijl dit systeem ook kwetsbaarheden bevat en onderdeel is van het datalek?
De GGD heeft mij gemeld dat er geen reden is om aan te nemen dat CoronIT inherent onveilig is. Het kwetsbare zit meer in het gebruik. Om die reden is bijvoorbeeld de printfunctionaliteit uitgezet en wordt automatische en continue monitoring van de logging voorbereid. Ten aanzien van de vaccinaties, zou uitwijken naar een ander systeem een langere ontwikkeltijd gevergd hebben waardoor starten met (afspraken maken voor) vaccineren ernstig in het gedrang zou komen.

353. Hoe wordt dit systeem verbeterd teneinde datalekken te voorkomen?
De GGD heeft mij gemeld dat CoronIT geen exportfunctionaliteit heeft. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Daarnaast wordt automatische en continue monitoring van de logging voorbereid.

Vragen en opmerkingen van de PvdA-fractie

De leden van de PvdA-fractie hebben met grote zorgen kennisgenomen van de privacy problemen rondom de coronasystemen van de GGD. Dat criminelen toegang hebben kunnen krijgen tot adres, BSN en medische gegevens van miljoenen Nederlanders is zeer kwalijk. Dat de GGD signalen hierover al maanden onder het tapijt heeft geschoven, vinden genoemde leden ronduit schandalig. Draagvlak voor de aanpak van het bron- en contactonderzoek en vertrouwen in het handelen van de overheid zijn cruciaal in de bestrijding van het coronavirus. Hoe kan, áls straks de maatregelen eindelijk versoepeld kunnen worden, een volgende golf voorkomen worden als mensen zich niet meer durven te laten testen en niet meer mee willen werken aan bron- en contactonderzoek?

354. Welke keuzes liggen volgens de Minister ten grondslag aan de gekozen datasystemen?
De GGD heeft mij gemeld dat HPZone het enige systeem was dat voorhanden was om in maart 2020 snel aan de slag te gaan. GGD'en hebben aan het begin geconstateerd dat HPZone niet aan de eisen van deze tijd voldoet, hebben aanpassingen gepleegd, maar wisten ook dat een nieuw systeem nodig was.
Bij aanvang van de ontwikkeling en het gebruik van CoronIT ging het over een substantieel kleinere gebruikersomvang. Gedurende de verdere opschaling van het test- en traceerbeleid is de robuustheid en schaalbaarheid van het systeem continu punt van aandacht geweest. Daarbij is een continue afweging gemaakt tussen aanpassingen om beleidswijzi-

gingen te ondersteunen en aan gebruikersvriendelijkheid, bedrijfscontinuïteit en privacy.

355. Welke keuzes liggen ten grondslag aan het aantal gegevens dat werd bewaard?
De GGD heeft mij gemeld dat in CoronIT naam, adres, woonplaats, telefoonnummer/e-mailadres, BSN, geslacht, geboortedatum, test- en/of vaccineerafspraken en testresultaten staan. In HPZone staan naam, adres, woonplaats, telefoonnummer, geslacht, geboortedatum en BSN van een persoon. Verder wordt in HPZone ook de informatie uit de bron- en contactonderzoek gesprekken vastgelegd. Dit is onder andere welke COVID-19 klachten de persoon in kwestie heeft, waar iemand is geweest en met wie hij/zij in contact is geweest. Ook wordt informatie vastgelegd van bron(nen) en nauwe contacten. De GGD is op basis van de Wet op de Geneeskundige Behandelovereenkomst (WGBO) ook verplicht om bepaalde gegevens vast te leggen.

356. En welke privacy voorwaarden waren aan de gekozen systemen verbonden?
De GGD heeft mij gemeld dat de gegevens zoals geregistreerd in CoronIT zijn opgenomen in de privacyverklaring CoronIT. Hetzelfde geldt voor HPZone, deze zijn terug te vinden in de privacyverklaring van bron- en contactonderzoek in het kader van COVID-19.

357. Sinds wanneer was de AP op de hoogte van de problemen?
In september 2020 zijn de problemen omtrent de coronatestlijn ontdekt en aan het licht gebracht door Nieuwsuur. Het lijkt daarbij te gaan om verwerkingen die uitsluitend plaatsvinden in het systeem CoronIT. Naar aanleiding daarvan heeft de AP de GGD ter verantwoording geroepen.
In november 2020 werd melding gemaakt van een datalek waarbij 2 personen betrokken waren. Het datalek had betrekking op CoronIT. Naar aanleiding van vragen van de AP zijn maatregelen toegezegd door de GGD.
In januari 2021 is vervolgens een nieuwe datalekmelding gedaan, die uiteindelijk drie systemen betrof: CoronIT, HP Zone, en HP Zone Lite (het systeem dat het bron- en contactonderzoek ondersteunt). Naar aanleiding van die melding heeft de AP het toezicht verder verscherpt. Ook omdat bleek dat het interne toezicht vanuit de GGD en de eerder toegezegde maatregelen blijkbaar nog onvoldoende effect sorteerden.

358. Welke stappen heeft de AP vanaf 16 september 2020 gezet?
359. In hoeverre was de Minister daarvan op de hoogte?
N.a.v. de berichtgeving van Nieuwsuur van 16 september jl. is GGD ter verantwoording geroepen. GGD is uitdrukkelijk gewezen op hun wettelijke verplichting te zorgen dat de gegevens van burgers goed beveiligd zijn. De AP heeft aangegeven dat de GGD risico's in kaart moet brengen en waar nodig maatregelen moet treffen om bestaande (en toekomstige) problemen op te lossen. Daarbij is aangegeven dat de AP handhavend kan optreden indien nieuwe signalen/klachten daartoe aanleiding geven. In november heeft de AP wederom contact gehad met de GGD ditmaal in verband met een datalek waarbij er gegevens van 2 personen waren gelekt. De AP heeft vragen gesteld en de GGD heeft maatregelen aangekondigd, die eind 2020/begin 2021 ingevoerd zouden worden.
Na de onthullingen in januari door RTL en een nieuwe melding van een datalek verscherpt de AP het toezicht. Want prioriteit is nu, dat op dit moment de gegevens goed beschermd gaan worden om het vertrouwen te herstellen. Het werk van de GGD mag niet in gevaar komen, doordat mensen twijfelen zich te laten testen. Om die reden heeft de AP het toezicht geïntensiveerd en worden ook onderzoeksactiviteiten verricht.

360. De leden van de PvdA-fractie vragen de Minister vanaf wanneer hij weet van mogelijke lekken in de datasystemen en vanaf welk moment deze problemen bij de GGD zelf bekend waren.
De signalen over de toegang van medewerkers van het callcenter dat testafspraken inplant en uitslagen terugkoppelt zijn voorzover ik kan nagaan bij mij en medewerkers van het ministerie bekend geworden naar aanleiding van de publicatie van Nieuwsuur op 16 september. Ik heb uw Kamer in antwoord op schriftelijke vragen van de leden Hijink (SP) en Ellemeet, Smeulders en Buitenweg (GroenLinks) hierover geïnformeerd, en daarbij aangegeven welke maatregelen de GGD GHOR al sinds de start van het traject heeft getroffen om de privacy en vertrouwelijkheid van persoonsgegevens te borgen.

361. Wat is vanaf welk moment ondernomen om mogelijke lekken in de digitale systemen spoedig in zicht te krijgen om deze zodoende snel te kunnen verhelpen?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

362. Hoeveel meldingen omtrent privacy problemen hebben het Ministerie van VWS in totaal bereikt?
Ik verwijs u graag naar het antwoord op 260.

363. Vanaf wanneer zijn deze meldingen binnen de GGD intern gedaan?
Ik verwijs u graag naar het antwoord op 260.

364. Vanaf wanneer waren deze meldingen bij het Ministerie van VWS bekend?
Ik verwijs u graag naar het antwoord op vraag 260

365. Vanaf wanneer heeft het Ministerie van VWS hulp aangeboden om deze problemen te verhelpen? In welke vorm heeft het Ministerie van VWS deze hulp aangeboden? Wat is door de desbetreffende instanties met deze hulp gedaan?
Het Ministerie van VWS heeft in december samen met de GGD GHOR een risicoanalyse laten doen. Op basis daarvan wordt nu een verbeterplan gemaakt dat ik binnenkort verwacht te ontvangen.

366. Indien het Ministerie van VWS al vroegtijdig op de hoogte was van de zorgen die er waren omtrent het waarborgen van de privacy bij de coronasystemen, waarom is dan besloten dezelfde systemen eveneens in te zetten bij het vaccinatieprogramma?
Zie het antwoord op 341.

367. Heeft de Minister overwogen om eerst de privacy problemen te achterhalen en te verhelpen, alvorens een definitieve keuze te maken voor het in te zetten registratiesysteem bij het vaccineren?
De GGD heeft mij gemeld dat er aanvullende eisen zijn gesteld aan de leverancier op het gebied van capaciteit van de applicatie en het team dat de applicatie ondersteunt. Daarnaast is een aparte DPIA uitgevoerd en zijn speciale autorisatierollen voor vaccineren ontworpen en geïmplementeerd, zodat medische gegevens naar behoren zijn afgeschermd.

368. Ook vragen de leden van de PvdA-fractie de Minister hoe het kan dat binnen de GGD interne meldingen over privacy problemen weggewuifd werden?
De GGD heeft mij gemeld dat er één signaal formeel is binnen gekomen bij GGD GHOR Nederland van medewerkers, hierop is gereageerd en geacteerd. Op dit moment is er geen totaaloverzicht van klachten of

meldingen door medewerkers die ingediend zijn bij GGD'en en de opvolging daarvan.

369. Heeft de zelfstandige positie van de GGD een rol heeft gespeeld in het tempo waarin de zorgen omtrent de privacy het Ministerie van VWS hebben bereikt?
GGD GHOR Nederland en de GGD'en informeren mij niet over individuele meldingen of klachten over IT-systemen. Deze worden in de organisaties zelf opgepakt.

370. De leden van de PvdA-fractie vragen de Minister hoeveel mensen exact toegang hebben gekregen tot de paspoort- en identiteitsgegevens die zijn opgeslagen in CoronIT?
De GGD heeft mij gemeld dat GGD-Medewerkers die betrokken zijn bij testen en vaccineren toegang tot persoonsgegevens hebben in CoronIT. GGD-medewerkers die betrokken zijn bij bron- en contactonderzoek hebben toegang tot HPZone (Lite). Samen met de medewerkers van gecontracteerde partijen gaat het om 26.000 medewerkers die toegang hebben tot CoronIT en 20.000 tot HPZone (Lite).

371. Waarom wordt een BSN opgeslagen? Waarom is dit nodig voor het systeem van testen en/of vaccineren?
Ik kan de leden van de PVDA-fractie melden dat de GGD'n het testen en vaccineren verrichten als zorgverlener. De GGD heeft in het kader van testen een behandelovereenkomst met de betrokkene. In dit kader heeft de GGD als zorgaanbieder de verplichting het Burgerservicenummer te registreren van betrokkene en ook een medisch dossier bij te houden op grond van de Wet op de Geneeskundige behandelingsovereenkomst (Wgbo), waarin op basis van BSN geregistreerd moet worden. Dit is noodzakelijk om te waarborgen dat de in het kader van de verlening van zorg te verwerken persoonsgegevens op die cliënt betrekking hebben.

372. Hoe vaak is de exportfunctie in CoronIT in totaal gebruikt?
CoronIT heeft geen exportfunctionaliteit.

373. Is controleerbaar welke medewerkers gebruik hebben gemaakt van deze exportfunctie?
De GGD heeft mij gemeld dat CoronIT geen exportfunctionaliteit heeft. Logging van zoekopdrachten en toegang vindt plaats.

374. Hoe kan het dat de exportfunctie in het systeem tot deze week beschikbaar bleef? Waarom is daar niet al in september naar gekeken?
De GGD heeft mij gemeld dat sinds de zomer van 2020 diverse maatregelen zijn getroffen om het toegangsbeheer te verscherpen en om controles uit te voeren op de toegang tot en het gebruik van persoonsgegevens. Gedurende de gehele periode zijn autorisaties verscherpt, waarbij bij CoronIT in eerste instantie aandacht is uitgegaan naar de scheiding van rollen en inrichting van de rollen, vervolgens naar de logging van activiteiten. Met het oog op dat laatste is een project gestart om geautomatiseerde controle hierop plaats te laten vinden.
Voor HPZone (Lite) zijn extra logging functionaliteiten ingericht, is een risicoanalyse uitgevoerd om verdere risico's te identificeren, zijn de aanbevelingen opgepakt en vertaald in een aantal maatregelen, is een project gestart om toegang beter te loggen en monitoren. Verder verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

375. Zijn of worden mensen waarvan mensen hun gegevens zijn gelekt persoonlijk op de hoogte gebracht? Zo nee, wanneer gaat dat gebeuren?

De GGD heeft mij gemeld dat op dit moment onduidelijk is wat de omvang is van het aantal data dat gestolen is. Dat is onderdeel van het politieonderzoek.
De GGD heeft mij gemeld dat wanneer bekend is van welke personen informatie gestolen is, de GGD hen zal informeren. Burgers moeten te allen tijde kunnen vertrouwen dat medische gegevens veilig worden gedeeld en bewaard, juist vanwege het privacygevoelige karakter van deze gegevens. Incidenten als deze zijn zeer ernstig voor de mogelijke slachtoffers, het vertrouwen heeft schade opgelopen en dat betreur ik.

376. Klopt het dat de GGD zo snel mogelijk wil stoppen met het gebruik van een van de softwaresystemen waaruit grote hoeveelheden persoonsgegevens zijn gestolen. Zo ja, waarom gebeurt dat nu pas? Per wanneer gaat dit gebeuren?
GGD GHOR Nederland heeft mij gemeld dat zij voor het bron- en contactonderzoek overgaan op een nieuwe voorziening. Dat zal versneld gaan gebeuren. Het exacte moment is nog niet bekend; de activiteiten zijn gericht op een overgang in maart. De noodzakelijke functionaliteit voor COVID-19-bestrijding dient aanwezig te zijn.

377. Is de Minister gedurende de verdere bestrijding van de coronacrisis voornemens anders regie te voeren met betrekking tot de GGD?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

378. Op welke wijze is de Minister voornemens om het vertrouwen in de systemen van de GGD te herstellen?
Voor het antwoord op deze vraag verwijs ik u naar mijn brief die ik op 2 februari aan uw Kamer heb gestuurd.

379. Waarom stelt de Minister dat er volcontinue en volautomatisch wordt gecontroleerd op het gebruik van de GGD-systemen? Is dit werkelijk gebeurd? Zo ja, hoe kan het datalek dan zijn ontstaan? Of zijn enkel steekproeven uitgevoerd?
Tijdens het mondelinge vragenuur van afgelopen dinsdag 26 januari heb ik gezegd dat de GGD sinds de start van de pandemie «continu het gebruik van de systemen» controleert. Dit heeft ten onrechte bij sommigen de indruk gewekt dat er nu reeds sprake is van een volautomatische controle, terwijl de GGD tot nu toe structureel steekproefsgewijs controleert. Ik heb daarna gezegd dat «die controles ook worden geautomatiseerd, zodat ze volcontinu kunnen worden uitgevoerd», en had daarbij voor de helderheid beter kunnen aangeven dat dit pas in maart gerealiseerd zal zijn. Ik betreur dat hierover misverstanden zijn ontstaan en zet dit in de brief aan uw Kamer inzake het datalek bij de GGD recht.

380. Wat hield de risicoanalyse die in december is uitgevoerd precies in?
De GGD heeft mij gemeld dat risicoanalyses vertrouwelijke informatie bevatten en kunnen om veiligheidsredenen niet worden gedeeld met de Kamer.

381. Welke maatregelen zijn vanaf december aanvullend genomen?
GGD GHOR Nederland heeft mij gemeld dat zij bezig waren met de ontwikkeling van de automatische en continue monitoring. Deze werkzaamheden zijn vertraagd toen de vaccinatie-opdracht versneld bij de GGD'en belegd werd en daarvoor de benodigde functionaliteiten in de systemen ingeregeld dienden te worden.
Na het onderzoek van RTL zijn aanvullende maatregelen genomen ten aanzien van export- en printfunctionaliteiten en ten aanzien van de logging.

382. In hoeverre voldeed het systeem in september aan de AVG? In hoeverre voldoet het nu? Wat is sindsdien precies gewijzigd?
De GGD heeft mij gemeld dat zij vanaf het begin bij CoronIT rekening werd gehouden met alle eisen en verplichtingen van de AVG. Dit is nu niet anders. Wel zijn naar aanleiding van diverse incidenten bestaande maatregelen verscherpt. Hier kan gedacht worden aan zero tolerance beleid voor onrechtmatige inzage van dossiers, aanscherping van trainingen, (verdere) aanscherping van autorisaties en het uitschakelen van accounts van medewerkers van landelijke callcenter tussen 22.00 en 07.00, zodat zij geen toegang hebben buiten werktijden, en er wordt gewerkt aan het inrichten van continue automatische controle van logging.

383. In hoeverre voldeed het systeem in september aan de Nederlandse Norm (NEN) 7510, de norm voor informatiebeveiliging in de zorg. In hoeverre voldoet het nu? Wat is sindsdien precies gewijzigd?
De GGD heeft mij gemeld dat CoronIT is ingericht en werkt langs de lijn van NEN-7510. GGDGHOR Nederland bereidt zich voor op certificering van NEN7510.

Vragen en opmerkingen van de 50PLUS-fractie

De leden van de 50PLUS-fractie hebben kennisgenomen van de berichtgeving rondom het datalek in het GGD-systeem en hebben in dit kader de volgende vragen.

384. De Minister heeft aangegeven dat er toezicht is en er gecontroleerd wordt of medewerkers geen persoonsgegevens kopiëren. Kan de Minister aangeven hoe die controle eruitziet?
De GGD heeft mij gemeld dat tot nu toe steekproefsgewijze controle van de logging heeft plaatsgevonden. Gespecialiseerde externe teams doen op dit moment forensisch onderzoek naar de logging (de handelingen die in de GGD-systemen verricht zijn). En tot de start van automatisch en continu monitoren, blijven deze gespecialiseerde externe teams voor de GGD'en de loggings controleren.

385. Klopt het dat de gegevens van mensen die zich hebben laten testen vanaf het begin van de corona-uitbraak zijn opgeslagen? Zo ja, waarom worden de gegevens na de uitslag van de test niet vernietigd? Welke gegevens worden precies geregistreerd?
De GGD heeft mij gemeld dat zij zich aan de wettelijke termijnen die hiervoor gelden. Zij verwijderen de persoonsgegevens als deze niet langer noodzakelijk zijn, met een maximale bewaartermijn van 5 jaar. De GGD'en bewaren de persoonsgegevens in ieder geval voor de gehele duur van de pandemie. De GGD heeft een wettelijke bewaarplicht van bepaalde gegevens. Dus per geval zal gekeken moeten worden wat er mogelijk is.

386. Klopt het dat veel medewerkers van de GGD bij indiensttreding geen VOG hebben hoeven overhandigen? Kan de Minister aangeven hoe dit komt? Waarom heeft de Minister tijdens het vragenuur van 26 januari jl. aangegeven dat alle medewerkers van de GGD een VOG hebben moeten aanvragen? Heeft de Minister zicht op hoeveel medewerkers bij de GGD op dit moment zonder VOG werken en in het verleden persoonsgegevens hebben verwerkt?
De GGD heeft mij gemeld dat medewerkers van GGD'en en externe partijen een Verklaring Omtrent het Gedrag (VOG) moeten aanleveren. Gegeven de snelheid waarmee de GGD'en en GGD GHOR Nederland hun personele capaciteit moesten uitbreiden, kunnen zich situaties hebben voorgedaan waarin medewerkers wel toegang hadden tot systemen, maar nog geen VOG hadden overlegd.

387. Kan de Minister aangeven welke maatregelen hij neemt om te zorgen dat voor alle medewerkers van de GGD die met persoonsgegevens werken, zo snel mogelijk een VOG wordt aangevraagd?
GGD GHOR Nederland en de GGD'en hebben mij gemeld dat zij willen dat elke medewerker een VOG overlegt en een geheimhoudingsverklaring ondertekent. GGD GHOR Nederland zal de regionale GGD'en en gecontracteerde partijen opnieuw vragen daarvoor zorg te dragen.

388. Klopt het dat er mensen met een strafblad werkzaam zijn bij de GGD?
De GGD heeft bevestigd dat een VOG wordt verstrekt op basis van een toetsing op het profiel dat voor de betreffende functie is vastgesteld. Het kan zijn dat betrokkene veroordeeld is voor strafbare feiten die niet relevant zijn voor de functie waarvoor de VOG is aangevraagd.

389. Wat gebeurt er met de gegevens die commerciële teststraten moeten aanleveren aan de GGD? Worden deze gegeven ook bewaard? Zijn deze gegevens ook inzichtelijk voor iedereen? Is er toezicht op hoe die commerciële aanbieders omgaan met persoonsgegevens? Zijn er signalen dat bij die aanbieders persoonsgegevens worden verhandeld? Is er zicht op of medewerkers van commerciële aanbieders wél allemaal een VOG hebben?
De GGD heeft mij gemeld dat bij een positieve uitslag elke andere organisatie verplicht is om dit te melden aan de GGD. De gegevens worden opgenomen in HPZone.
De Inspectie Gezondheidszorg en Jeugd houdt toezicht op commerciële aanbieders.

390. Kan de Minister aangeven wanneer hij voor het eerst heeft gehoord dat er een probleem was met het systeem? Welke maatregelen heeft hij toen genomen? Kan de Minister aangeven wanneer de GGD het probleem voor het eerst heeft gemeld en aan wie dit was?
391. Kan de Minister aangeven wat er intern bij de GGD is gebeurd met alle signalen die medewerkers hebben gegeven over het datalek in het softwaresysteem?
390 en en 391: De signalen over de toegang van medewerkers van het callcenter dat testafspraken inplant en uitslagen terugkoppelt zijn voorzover ik kan nagaan bij mij en medewerkers van het ministerie bekend geworden naar aanleiding van de publicatie van Nieuwsuur op 16 september. Ik heb uw Kamer in antwoord op schriftelijke vragen van de leden Hijink (SP) en Ellemeet, Smeulders en Buitenweg (GroenLinks) hierover geïnformeerd, en daarbij aangegeven welke maatregelen de GGD GHOR al sinds de start van het traject heeft getroffen om de privacy en vertrouwelijkheid van persoonsgegevens te borgen.
Voorts verwijs ik u naar het antwoord op vraag 260.

392. Kan de Minister aangeven door welke partij het softwaresysteem is getoetst op veiligheid? Is er een BIT-toets gedaan op het systeem?
De GGD heeft mij gemeld dat van het begin van het testen gespecialiseerde interne en externe teams betrokken zijn bij de externe veiligheid van de systemen. Het BIT heeft geen toets uitgevoerd.

393. Wie is verantwoordelijk voor de veiligheid van het systeem?
De GGD'en en GGD GHOR Nederland zijn verantwoordelijk voor de veiligheid van de systemen.

394. Hoe wordt de veiligheid getoetst, bewaakt en wie heeft toegang?
De GGD heeft mij gemeld dat van het begin van het testen gespecialiseerde interne en externe teams betrokken zijn bij de externe veiligheid van de systemen. In opdracht van GGD GHOR Nederland wordt op dit moment forensisch onderzoek uitgevoerd door een gespecialiseerd extern

team naar onze logging (de handelingen die in het systeem verricht zijn). Er worden op dit moment ook andere wijzigingen in de systemen aangebracht. Er wordt gewerkt aan de implementatie van automatische en continue monitoring die eind maart gereed zal zijn. Tot dat moment controleren gespecialiseerde interne en externe teams de logging.

395. Kan de Minister aangeven waarom er een exportfunctie in het systeem zit?
De GGD heeft mij gemeld dat de exportfunctie in HPZone nodig is zodat GGD-epidemiologen rapportages kunnen maken op basis van datasets en t.b.v. clusteranalyse en uitbraakbestrijding. Daarnaast is de functie nodig zodat GGD'en analyses kunnen maken ten behoeve van rapportages voor gemeenten in hun GGD-regio.
CoronIT heeft geen exportfunctionaliteit. De printfunctionaliteit is direct uitgezet toen de datadiefstal aan het licht kwam. De printfunctie was met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is. Het uitzetten van de printfunctionaliteit levert geen problemen op voor het operationeel proces.
HPZone heeft zowel een export- als een printfunctionaliteit. De exportfunctionaliteit is nodig om datasets te creëren voor statistische analyses ten behoeve van de teams infectieziekte bestrijding. De functie kan daarnaast worden gebruikt om databestanden te genereren voor opslag in een beveiligd datawarehouse. De exportfunctionaliteit wordt ook gebruikt om werk te verdelen over de medewerkers.
Met de printfunctionaliteit kan de medewerker de informatie die op dat moment zichtbaar is op de pagina, opslaan in een PDF. De printfunctionaliteit wordt met name gebruikt om dossiers over te dragen aan een andere GGD. De functionaliteit kan ook gebruikt worden om een werklijst te printen.
De exportfunctionaliteit is maandag 25 januari 2021 uitgezet en inmiddels weer voor een beperkt aantal medewerkers beschikbaar. Uitzetten van de printfunctionaliteit heeft grote gevolgen voor de werkzaamheden. In eerste instantie is deze functionaliteit daarom niet uitgezet. Op zaterdag 30 januari 2021 is dat alsnog gebeurd. Als gevolg van deze maatregelen kunnen de medewerkers nu minder efficiënt werken.

396. De Minister gaf in het vragenuur van 26 januari jl. aan dat het systeem aan de NEN7510 norm voldoet? Klopt dit?
Ik verwijs u naar de brief die ik uw Kamer toezend deze week, waarin ik reflecteer op mijn uitspraken.

397. Speelt het Nationaal Cyber Security Centrum in dit kader nog een rol?
De Wet beveiliging netwerk- en informatiesystemen (WBNI) ziet primair op vitale aanbieders en de rijksoverheid en regelt de taken van het Nationaal Cyber Security Centrum (NCSC) daarin. De GGD-en vallen niet onder die categorieën. Uiteindelijk is het aan de aanbieders van diensten zelf, i.c. GGD-en, om voor hun basisbeveiliging te zorgen, ook als ze niet onder de WBNI vallen.
Z-CERT heeft vooruitlopend op de daadwerkelijke aansluiting van de GGD-sector op hun dienstverlening later dit jaar afgesproken, alvast te beginnen met het delen van informatie over informatiebeveiliging en het aanbieden om bestaande informatiebeveiliging te reviewen.

398. Is de AP op enigerlei wijze betrokken bij de inrichting van het systeem? Is aan hen advies hieromtrent gevraagd?
Dit is niet de positie van de AP. De AP is toezichthouder waar de GGD wettelijk verantwoordelijk is voor de beveiliging van de gegevens die het verwerkt.

Het is aan de GGD om een DPIA te maken. Daarin komen de risico's aan de orde bij gegevensverwerking. Alleen als de GGD inschat dat risico's niet gemitigeerd kunnen worden door aanvullende maatregelen en er onverantwoorde risico's overblijven, dan moet de GGD de AP voorafgaand raadplegen. Dat is niet gebeurd.

399. Wat wordt er inmiddels gedaan om de schade te beperken en kan achterhaald worden aan wie gegevens zijn gelekt c.q. verkocht?
Hierover kunnen wij voor nu geen uitspraken doen, dit is onderdeel van het onderzoek van politie en justitie.