Q&A WOB-/WOO-VERZOEK
De termijn om aan het Woo-verzoek te voldoen loopt t/m woensdag a.s. (1 juni). De publicatie van in elk geval de GGD GHOR-stukken zal dan plaatsvinden. Ook zullen veel GGD'en dan eigen stukken publiceren. Onderstaand een woordvoeringslijn vanuit GGD GHOR Nederland die ook kan helpen bij het beantwoorden van vragen over het proces, onze mening over ICAM, de inhoud van documenten die we openbaar maken. De regionale GGD'en beantwoorden vragen die zij hierover krijgen zelf. Als er inhoudelijke vragen zijn over GGD GHOR-stukken of over dit proces dan kan GGD GHOR Nederland deze vragen beantwoorden. Belangrijkste is dat we woordvoering onderling afstemmen, zodat we elkaar niet verrassen of in verlegenheid brengen. En te concentreren op de eigen afwegingen en niet te oordelen over anderen en/of te reageren op mogelijke verschillen. Bij twijfel graag overleggen met woordvoering landelijk. (Jacqueline Toonen: 06-15189751).

UITLEG WERKWIJZE AFHANDELING WOB-/WOO-VERZOEK
We maken onderscheid tussen het proces voor:
A) de documentatie die GGD GHOR NL voor GGD'en verzamelt: dit zijn de stukken die GGD GHOR NL heeft gedeeld met alle GGD'en; en
B) de documentatie die GGD'en zelf verzamelen. Uiteraard worden alleen de stukken waarin VWS belanghebbende is voorgelegd.

Samenvatting proces A
- De GGD GHOR-documentatie is beoordeeld op i) binnen de scope van het Wob/Woo-verzoek valt; (ii) of een document potentieel schadelijk is, en zo ja; (iii) welke uitzondering eventueel van toepassing is op het betreffende (onderdeel van) document en welke motivering daarbij past. Afhankelijk van die beoordeling kan de verstrekking van documenten achterwege blijven, dan wel kunnen onderdelen daarvan worden gelakt.
- GGD Zeeland is de partij die de GGD GHOR-documentatie online plaatst, zodat andere GGD'en alleen maar naar die publicatie en de motivering van GGD Zeeland hoeven te verwijzen. De beoordeling van die documenten (wel/niet/gedeeltelijk verstrekken) wordt daarmee in principe door iedereen overgenomen.

Samenvatting proces B
- Voor regionale GGD-stukken maken GGD'en zelf een afweging, aan de hand van een referentiebeoordeling die is uitgevoerd op het dossier van GGD Zeeland. Dit dossier biedt een voorbeeld van welke (type) stukken wel/niet/gedeeltelijk openbaar moeten worden gemaakt en waarom.
- Het kan zijn dat GGD'en de deadline van 1 juni niet halen, of slechts een gedeelte van de stukken kunnen verstrekken. Ofwel door tijdnood, ofwel omdat een andere partij nog om een zienswijze moet worden gevraagd op de publicatie van de stukken (dwz: bij een

zienswijze wordt een partij die in stukken genoemd wordt gevraagd of/waarom deze er bezwaar tegen heeft dat de info in een bepaald document openbaar wordt.) In dat geval zullen zij deelbesluiten gaan nemen. De rest volgt dan later op een door de regionale GGD te bepalen tijdstip.

Q&A WOO-VERZOEKEN

Wat is er aan de hand?
Op 15 februari 2022 kreeg elke GGD een Wob-verzoek (vanaf 1 mei 2022 heet dit een Wet Open Overheid-verzoek) van Stichting ICAM naar aanleiding van de datadiefstal uit CoronIT. Elke GGD heeft een eigen verantwoordelijkheid en bevoegdheid om invulling te geven aan het Woo-verzoek. GGD GHOR Nederland kreeg ook dit Wob-verzoek maar valt niet onder de werkingssfeer en gaat daardoor zelf geen stukken verstrekken. Wel coördineert GGD GHOR Nederland op verzoek van de DPG'en de afhandeling van dit Woo-verzoek en wordt daarbij juridisch bijgestaan door van Doorne. Dat doet GGD GHOR Nederland vanwege het belang van alle GGD'en om dit verzoek op consistente wijze te behandelen. De termijn om aan het Woo-verzoek te voldoen loopt t/m woensdag 1 juni 2022. De publicatie van in elk geval de GGD GHOR-stukken (via GGD Zeeland) zal dan plaatsvinden. Ook zullen veel GGD'en nog eigen stukken publiceren.

Stichting ICAM?
Stichting ICAM zegt op te komen voor de belangen van groepen mensen die schade lijden door toedoen van grote organisaties. Een procesfinancier (Liesker Procesfinanciering) financiert de collectieve rechtszaak die ICAM wil aanspannen. Burgers kunnen zonder kosten deelnemen, op basis van een no cure no pay-regeling. In ons geval stelt ICAM op te komen voor burgers die ten tijde van de datadiefstal (januari 2021) in de corona-systemen stonden geregistreerd. Deze burgers zouden onvoldoende beschermd zijn tegen inbreuken op hun privacy door "de overheid". De zaak wordt inhoudelijk behandeld door een team van het bureau SOLV Advocaten onder leiding van Douwe Linders. De procesfinancier krijgt een vergoeding voor zijn kosten als de zaak slaagt. Deze vergoeding bedraagt 20% van de schadevergoeding die Stichting ICAM voor gedupeerden weet te innen en is gemaximeerd op vijf keer de door de procesfinancier geïnvesteerde som.

Stichting ICAM spreekt het ministerie van Volksgezondheid, Welzijn en Sport (VWS) aan: "Gedurende de corona pandemie hebben de GGD'en hun uiterste best gedaan om alles in goede banen te leiden. Het ging echter mis bij het beveiligen van de IT-systemen waarin persoonsgegevens van 6,5 miljoen Nederlandse burgers zijn opgeslagen. Het ministerie van VWS had de leiding over de

bestrijding van de corona pandemie en heeft opdracht gegeven tot de ingebruikname van de slecht beveiligde IT-systemen."

Werken jullie mee aan de WOO-verzoeken van Stichting ICAM?
Stichting ICAM heeft verschillende verzoeken om informatie bij de GGD'en en GGD GHOR Nederland neergelegd, waaronder een Wob verzoek d.d. 15-02. Dit verzoek heeft zij overigens ook aan de veiligheidsregio's en gemeenten gedaan. De GGD'en werken mee aan dit Wob verzoek en trachten zo zorgvuldig mogelijk dit verzoek af te wikkelen. Vanwege de grote hoeveelheid gevraagde documentatie is uitstel aan ICAM gevraagd tot 1 juni. Op die datum zal een (groot) deel van de gevraagde documentatie verstrekt worden.

Heel veel documenten worden niet verstrekt/zijn grotendeels weggelakt. Waarom is dat?
We hebben met de grootst mogelijke zorgvuldigheid invulling proberen te geven aan het Wob verzoek. Gezien de enorme reikwijdte van het verzoek zullen zeer veel documenten verstrekt worden. De documenten die niet verstrekt worden vallen ofwel niet onder de reikwijdte van het verzoek of vallen onder een uitzonderingsgrond zoals gedefinieerd in de Woo. Onderdelen van documenten zijn gelakt conform de bepalingen daarover in de Woo.

Geven we zo niet onvoldoende openheid van zaken?
Als GGD zijn we meer dan bereid om openheid van zaken te geven. Vanuit die grondhouding hebben we het Wob verzoek van ICAM in behandeling genomen en bij iedere categorie van opgevraagde documenten beschouwd welke documenten onder de reikwijdte vallen en verstrekt dienen te worden.

Het decentrale systeem en de decentrale infrastructuur?
Het zal inmiddels niemand meer verrassen als we stellen dat de decentrale infrastructuur die de GGD'en kenmerkt, niet altijd even effectief was om een pandemie te bestrijden. Dat gold zeker ook voor de IT-systemen en datastromen waarlangs gewerkt is. Dat was echter hetgeen voor handen was en waarmee we gewerkt hebben teneinde besmettingen, ziekte en ziekenhuisopname zoveel mogelijk te voorkomen.

Wat vinden jullie van de massaclaim die Stichting ICAM heeft neergelegd?
GGD GHOR en GGD'en werden eind januari 2021 geconfronteerd met datadiefstal uit corona-systemen. Er is direct aangifte bij de politie en melding bij AP gedaan en de beveiliging van de systemen en data is verder geïntensiveerd. Een jaar politieonderzoek naar de verdachten van de datadiefstal toont aan dat gegevens van circa 1250 Nederlanders uit CoronIT gestolen zijn. Richting deze 1250 burgers

hebben wij een financieel gebaar gemaakt. Grootschalige databestanden noch de handel erin heeft de politie niet aangetroffen.
Wij zijn dan ook verbaasd dat stichting ICAM voor zo'n grote groep een schadevergoeding claimt. En verontwaardigd dat zij stelt dit vanuit een ideëel doel te doen; namelijk een betere beveiliging van de data van burgers. De stichting had er ons inziens beter aan gedaan haar zogenaamde ideële doel op een andere wijze te realiseren in plaats van met een massaclaim van 3,2 miljard met een keihard verdienmodel voor de procesfinancier daarachter. Het ideële doel, komen tot betere bescherming van persoonsgegevens, is bovendien al lang in het vizier van de GGD'en die daar het belang volledig van inzien. Immers hebben wij maar één doel; de gezondheid en veiligheid van Nederlanders bevorderen in én buiten crisistijd met alle waarborgen die daarbij horen.

Wat vinden jullie van dit soort claimstichtingen die duidelijk rendement willen zien op hun investeringen? Wij vinden het vooral van belang de daadwerkelijk betrokken burgers bij de datadiefstal te informeren en richting hen een financieel gebaar te maken. Dat past bij de maatschappelijke verantwoordelijkheid die we als organisatie hebben en voelen.

Wat hebben jullie gedaan na de ontdekking van de datadiefstal?
We hebben direct onderzoek ingesteld. Vervolgens contact opgenomen met de politie, aangifte gedaan en een melding gedaan bij de Autoriteit Persoonsgegevens. Ook hebben wij controles uitgevoerd in onze systemen én toegang verstrekt aan de politie om de opsporing zo goed mogelijk plaats te kunnen laten vinden. Wij controleren op verschillende manieren hoe onze medewerkers omgaan met de informatie in onze systemen. Indien we daar onregelmatigheden in zien, nemen we maatregelen. Ook beschermen we ons tegen aanvallen op onze systemen van buitenaf. De betrokkenen van wie de gegevens zijn ingezien, gestolen en mogelijk verkocht zijn allemaal via een brief door ons geïnformeerd.

Waarom starten jullie met een verouderd systeem?
In het voorjaar 2020 heerste angst in Nederland en werd alles in het werk gesteld om grip op het virus te krijgen. Het laten testen en uitvoeren van bron- en contactonderzoek waren dé instrumenten om het virus in beeld te krijgen en te bestrijden. Daar is alles voor in het werk gesteld. Snelheid was letterlijk van levensbelang. HPZone was het systeem dat voor handen was waarmee in Nederland al jaren werd gewerkt in het licht van infectieziektebestrijding. Een systeem dat niet ontwikkeld noch geschikt was voor dermate grote opschaling en gebruik. Een alternatief voor bron- en contactonderzoek was echter niet voor handen. In samenspraak met het RIVM en VWS is

daarnaast, toen duidelijk werd dat de GGD'en de uitvoering van het grootschalig testen op zich moesten nemen, CoronIT, ontwikkeld. Voor beide systemen is ervoor gezorgd dat alle medewerkers overal bij konden zodat indexen snel over hun testuitslag geïnformeerd konden worden en hun contacten konden worden geïnformeerd om zo de verspreiding van het virus in de kiem te smoren. Maximale opschaling was in die begin fase het devies. Later zijn hierop aanpassingen gepleegd waarbij onder andere rechten van medewerkers beperkt zijn en de monitoring is geïntensiveerd. En nog later is zelfs besloten om HPzone uit te faseren en te gaan vervangen door GGD Contact.
Alle medewerkers die toegang hadden tot deze systemen zijn geïnformeerd dat ze werken met gevoelige data, hebben scholing ontvangen, geheimhoudingsverklaring getekend, en wisten dat oneigenlijk gebruik strafbaar was. Sommige medewerkers/uitzendkrachten hebben toch misbruik gemaakt van de situatie deels uit naïviteit, deels heel bewust voor eigen gewin, dat is uiteraard zeer kwalijk.

Welke maatregelen hebben jullie genomen?
Export- en printfuncties zijn direct beperkt en de loggingprocedures zijn geïntensiveerd en aangescherpt, waarbij inmiddels ook geautomatiseerde controle plaatsvindt op de logging. Bij GGD Contact, het door het ministerie van VWS, GGD GHOR Nederland en alle GGD'en aangewezen vervangend systeem voor HPZone Lite, zijn informatiebeveiliging en privacy integrale onderdelen geweest van de ontwikkeling en implementatie. GGD GHOR heeft de Autoriteit Persoonsgegevens middels de door haar gevraagde voortgangsrapportage nader geïnformeerd over de verbeteringen die doorgevoerd zijn.

Kunt u garanderen dat de gegevens van mensen nu veilig bij u zijn?
Geen enkele organisatie kan 100% garantie geven. Dataveiligheid en privacy zijn integrale onderdelen van onze werkprocedures. Het is een doorlopend proces waarbij we continu de veiligheid van onze systemen analyseren en verbeteren. We spannen ons maximaal in om de data van alle Nederlanders goed te beschermen en beveiligen tegen onrechtmatige inzage en misbruik.

Klopt het dat de Autoriteit Persoonsgegevens (AP) onderzoek heeft gedaan n.a.v. de datadiefstal?
Ja, dat klopt. GGD GHOR Nederland heeft kennis genomen van de bevindingen die voortkomen uit het onderzoek van de AP naar de datadiefstal van begin 2021. Net als de AP is ook GGD GHOR Nederland van mening dat persoonsgegevens zo goed mogelijk moeten worden beschermd. GGD GHOR Nederland heeft dan ook werk gemaakt van de aanbevelingen van de AP en de AP daarvan in kennis gesteld.

Hoe stelt GGD GHOR Nederland vast dat de Autoriteit Persoonsgegevens (AP) geen handhavingsbevoegdheden gebruikt, waaronder het opleggen van een boete?
De AP heeft aan GGD GHOR Nederland aangegeven geen handhavingstraject te starten, maar vraagt wel om een voortgangsrapportage op te leveren. Deze rapportage is eind februari 2022 aan de AP verstrekt.

Welke conclusies trok de Autoriteit Persoonsgegevens (AP) in haar onderzoek?
De AP signaleerde op basis van uitgebreid en intensief onderzoek een aantal verbeterpunten. Zo kwam het onder meer met de aanbeveling om de toegangsbeveiliging en de autorisatieprocessen verder aan te scherpen en de afspraken tussen partijen inzake de informatiebeveiliging te verbeteren. Daarnaast deed de AP aanbevelingen ten aanzien van de beveiliging en de vervanging voor de systemen HPZone en HPZone Lite. Zie hier de link (klik hier) naar ons websitebericht van 9 november 2021.

Wat vinden jullie ervan dat er datadiefstal heeft plaatsgevonden?
We betreuren het dat er datadiefstal uit onze systemen heeft plaatsgevonden. Iedere dag werkten we met vele collega's om Nederlanders te testen, te vaccineren en bron- en contactonderzoek uit te voeren. Het waarborgen van de dataveiligheid is daar onlosmakelijk mee verbonden. Nederlanders moeten erop kunnen vertrouwen dat hun data bij de GGD-organisaties in veilige handen zijn. Het is ook goed dat er vanuit de rechter een krachtig signaal is uitgegaan naar diegenen die zich schuldig aan de datadiefstal hebben gemaakt. Wij tolereren niet dat medewerkers misbruik maken van het systeem waartoe ze voor hun werkzaamheden bij de GGD'en toegang hebben. Indien een overtreding ontdekt wordt, wordt hier direct op geacteerd hetgeen kan leiden tot aangifte en ontslag op staande voet.

Vragen over systemen

Uit welke systemen is er sprake geweest van datadiefstal?
Tot nu toe is uit politieonderzoek alleen gebleken dat er uit CoronIT gegevens gestolen zijn. Dit is het administratiesysteem voor het testen en vaccineren en de communicatie hierover. Dus wanneer u een afspraak maakt voor een COVID-19-test via het callcenter, de COVID-19-test website of een arts, komen uw persoonsgegevens in CoronIT. Ook, wanneer u een afspraak maakt voor een vaccinatie.

Zijn mijn gegevens wel veilig bij jullie?
Geen enkel IT-systeem is onfeilbaar. Wij doen alles wat in ons vermogen

ligt om ervoor te zorgen dat gegevens van mensen die zich laten testen of vaccineren in veilige handen zijn. Daarom hebben we ook na dit incident maatregelen genomen om dit soort incidenten in de toekomst te voorkomen. Het gaat om de volgende maatregelen:

- Wij hebben maatregelen genomen om te voorkomen dat GGD-medewerkers gegevens makkelijk uit de systemen kunnen halen zonder daartoe bevoegd te zijn;
- Wij hebben de politie de noodzakelijke toegang gegeven tot onze systemen om de daders op te sporen;
- Wij hebben onderzoek gedaan op internet naar mogelijk te koop aangeboden persoonsgegevens;
- Wij hebben een specialistisch team samengesteld en extra controlemaatregelen genomen. Zo kunnen we continu nagaan of onze medewerkers op een zorgvuldige manier omgaan met de persoonsgegevens.

Zijn de systemen voor testen, bron- en contact onderzoek en vaccineren strikt gescheiden?
Gegevens van testen en vaccineren bevinden zich in CoronIT. De medische gegevens die bij vaccinaties worden vastgelegd zijn afgeschermd en niet zichtbaar voor medewerkers die zich met testen bezighouden. Wel is er een koppeling waardoor een testuitslag altijd te zien is, wanneer iemand in het systeem kijkt bij een vaccinatie afspraak. Dit is zo ingericht omdat het nodig kan zijn om te bepalen of iemand gevaccineerd kan worden. De gegevens van het bron- en contactonderzoek bevinden zich in HPZone.

Hoeveel Nederlanders staan er in CoronIT en HPzone?
Op het moment dat de datadiefstal werd geconstateerd (januari 2021) stonden in CoronIT gegevens van circa ca. 5,5 miljoen mensen en in HPZone gegevens van circa 1 miljoen personen.

Hoeveel medewerkers hebben toegang tot CoronIT?
In totaal ging het in de piekperiode om ca. 35.000 medewerkers. Zowel bij de GGD'en als bij bedrijven die gecontracteerd zijn voor de COVID-19-bestrijding.

Wat doen de medewerkers in CoronIT en HPZone?
Medewerkers van het callcenter die telefoontjes ontvangen kunnen via CoronIT testafspraken en vaccinatieafspraken maken. Verder kunnen de medewerkers die uitgaande telefoontjes plegen de testuitslagen zien, zodat ze die kunnen meedelen. Bron- en contactonderzoekers leggen alle gegevens rondom een besmetting vast in HPZone.

CoronIT

Wat is er precies gestolen uit CoronIT?
Uit politieonderzoek naar de verdachten van de datadiefstal is gebleken dat de gegevens van circa 1.250 personen onbevoegd zijn ingezien, gestolen en mogelijk verkocht. Uit het onderzoek blijkt dat het gaat om gegevens van personen die bij een GGD een coronatest hebben laten doen of zich bij een GGD hebben laten vaccineren. Deze gegevens bevatten onder meer naam, geboortedatum, adres, telefoon, e-mailadres, Burgerservicenummer (BSN) en nationaliteit. De personen om wie het gaat zijn door ons geïnformeerd.

Is het normaal dat zoveel medewerkers toegang hebben tot deze gegevens? En, waarom is dit nodig?
Wij willen het coronavirus zo goed mogelijk bestrijden. Daarbij zijn veel medewerkers betrokken. Elke callcenter medewerker die telefoontjes aanneemt (inbound) moet afspraken kunnen maken. En iedere callcenter medewerker die mensen belt (outbound) moet uitslagen door kunnen geven als deze binnen zijn. Dit alles om te zorgen dat een besmet persoon zo snel mogelijk kennis heeft van diens besmetting en daarmee nieuwe besmettingen kan voorkomen.

Welke verbetermaatregelen zijn er genomen?
Direct na de datadiefstal in januari 2021 zijn er, zoals de Autoriteit Persoonsgegevens ook in haar eindbrief heeft vastgesteld, direct verdere verbetermaatregelen genomen ter bescherming van de persoonsgegevens die door de GGD-organisaties worden verwerkt in het kader van de bestrijding van de coronapandemie. De toegang tot de Corona applicaties is enkel en alleen mogelijk indien een medewerker getekend heeft voor zijn of haar (arbeids-)overeenkomst, een geheimhoudingsbeding en een door het ministerie van Justitie verstrekte Verklaring Omtrent Gedrag (VOG) heeft overlegd. Ook zijn de werkinstructies en de trainingen op het gebied van de verwerking en bescherming van persoonsgegevens verder aangescherpt. Om mensen goed te helpen is het noodzakelijk dat sommige medewerkers alle inwoners die in het systeem staan, kunnen opvragen. De gebruiker ziet alleen die gegevens die hij of zij op dat moment voor zijn werk nodig heeft. Wanneer een medewerker misbruik maakt van zijn of haar rechten geldt een zerotolerance beleid en zal, na onderzoek, aangifte bij de politie worden gedaan. Daarnaast zijn er verdere technische en functionele aanpassingen gedaan in de Corona-applicaties.

Wat betekent het beperken van de snelheid waarmee testen en bron- en contactonderzoek kan worden uitgevoerd?
Het testen en bron- en contactonderzoek loopt onverminderd door. Dat

is immers nodig om de pandemie te bestrijden. Wel hebben we een aantal extra waarborgen ingebouwd om datadiefstal te voorkomen. Deze waarborgen zijn echter niet van invloed op de doorlooptijd om een test- of vaccinatieafspraak te maken of de testuitslag te krijgen, noch op de doorlooptijd van het bron- en contactonderzoek.

HPZone

Waarom starten jullie met een verouderd systeem?
In het voorjaar 2020 heerste angst in Nederland en werd alles in het werk gesteld om grip op het virus te krijgen. Het laten testen en uitvoeren van bron- en contactonderzoek waren dé instrumenten om het virus in beeld te krijgen en te bestrijden. Daar is alles voor in het werk gesteld. Snelheid was letterlijk van levensbelang. HPZone was het enige systeem dat voorhanden was om in maart 2020 in vliegende vaart mee aan de slag te gaan. We hebben aan het begin geconstateerd dat HPZone niet geschikt was voor grote opschaling, maar een alternatief was niet voor handen. Bovendien bewust zo ingericht dat alle medewerkers overal bij konden zodat indexen en hun contacten snel geïnformeerd konden worden om verspreiding van het virus in de kiem te smoren. Er zijn aanpassingen gepleegd, maar we wisten ook dat een nieuw systeem nodig was.
Al die medewerkers zijn geïnformeerd dat ze werken met gevoelige info, hebben scholing ontvangen, geheimhoudingsverklaring getekend, wisten dat oneigenlijk gebruik strafbaar was.
Sommige medewerkers/uitzendkrachten hebben toch misbruik gemaakt van de situatie deels uit naïviteit, deels heel bewust voor eigen gewin, dat is uiteraard zeer kwalijk.

Klopt het dat er datasets uit HPZone zijn aangeboden?
We hebben signalen ontvangen dat datasets zouden zijn aangeboden, maar hebben niet kunnen vaststellen dat ze gestolen of verhandeld zijn. Een jaar na dato heeft de politie dat ook niet vast kunnen stellen. Uit politieonderzoek is alleen gebleken dat de gegevens van circa 1.250 personen onbevoegd zijn ingezien, gestolen en mogelijk verkocht.

Hoe kan het dat er sprake is van het exporteren van een dataset?
Voor CoronIT geldt hier het volgende: CoronIT beschikte niet over een exportfunctie, maar wel over een printfunctie om een lijst met personen die een afspraak had af te drukken. Die functie werd, afhankelijk van de locatie, voor verschillende doeleinden gebruikt. Onder andere door de portier/verkeersregelaar om te controleren of mensen die aankomen een afspraak hebben. Zo kon voorkomen worden dat mensen zonder afspraak in de keten kwamen en voor vertraging zorgen. Ook werd deze functie gebruikt om een noodlijst aan te leggen zodat in geval van uitval

van het systeem testgegevens op de lijst konden worden vastgelegd, zodat die na de storing geregistreerd konden worden.

Er zijn geen indicaties dat deze functie is misbruikt. Echter, omdat de kans bestond dat met het bekend worden van deze printfunctie het risico's op misbruik toe zou kunnen nemen, hebben we de printfunctie in CoronIT op maandag 25 januari 2021 uitgeschakeld. GGD'en kunnen als ze dat willen nu lijsten maken vanuit een beveiligde omgeving.

De exportfunctie van HP Zone maakte het mogelijk om een selectie van de gegevens in HP Zone te downloaden als lijst in bijvoorbeeld Microsoft Excel. De persoon die de export uitvoerde, kon variabelen selecteren (voorbeelden: leeftijd, postcode, testuitslag) en criteria toepassen om benodigde analyses te kunnen uitvoeren (voorbeeld: leeftijd >65). Deze lijsten werden gebruikt ten behoeve van de werkverdeling (door de supervisoren van het bron- en contactonderzoek), om analyses te doen en om rapportages te maken om zicht te houden op het virus (voorbeeld: clusteranalyse). Ook werden dergelijke lijsten gebruikt om de prestaties van de organisatie te monitoren (voorbeeld: analyse tijdigheid bron- en contactonderzoek ten behoeve van artsen, epidemiologen en data-analisten).

Klopt het dat die functie is uitgezet?
Ja, de belangrijkste exportmogelijkheden zijn uitgezet. En er zijn aanpassingen doorgevoerd in de overige exportmogelijkheden. De rechten voor gebruik van de resterende, benodigde exportfunctionaliteit zijn aan minder mensen toegekend op basis van beperktere rollen. Op 30 januari 2021 is de printfunctionaliteit in HPZone en HP Zone Lite uitgezet. Dit geldt voor zowel 'overzichten' als de individuele dossiers. Er kunnen geen persoonsgegevens worden geëxporteerd of geprint uit HPZone en HPZone Lite. Er geldt alleen een uitzondering voor het printen en exporteren van gepseunonimiseerde gegevens voor een zeer beperkt aantal daartoe geautoriseerde personen die de rol van "admin" of "coördinator" hebben", en waarbij de gepseunonimiseerde export voor statistische en onderzoeksdoeleinden is bedoeld. Deze prints en exports worden gelogd. Ook de weergave van de zoekresultaten is verder beperkt in de Corona applicaties. Bovendien kan een medewerker alleen toegang krijgen tot alle Corona applicaties indien zijn GGD-account geactiveerd is door de betreffende GGD.

HP Zone en HP Zone Lite. Wat is het verschil?
HPZone is een systeem dat wordt gebruikt voor infectiebestrijding van alle typen infectieziekten. Bij de uitbraak van het coronavirus is dit systeem ook hiervoor gebruikt. Met het uitbreiden van het aantal medewerkers, is HPZone Lite ontwikkeld om ervoor te zorgen dat zij alleen toegang hadden tot de COVID-19 data.

Waarom hebben jullie HP Zone Lite geïmplementeerd (in augustus 2020)?
HPZone Lite is bedoeld om grote aantallen medewerkers makkelijk te laten werken aan bron- en contactonderzoek. In de eerste golf liepen GGD-regio's over en konden andere GGD-regio's hen niet helpen. Dat hebben we opgelost in HPZone Lite, door het systeem zo in te richten dat GGD'en elkaar wel konden helpen. Hierdoor konden veel meer bron- en contactonderzoekers hun werk doen en kon het bron en contactonderzoek sneller worden opgestart zodat we voorkwamen dat positief geteste mensen en hun directe contacten weer anderen besmetten.

Kan een medewerker van GGD Groningen in een bron-en contactonderzoek casus van GGD Regio Utrecht?
Nee, GGD-medewerkers kunnen alleen bij de gegevens van hun eigen GGD. Het is wel zo 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 van die toegang is voor landelijke BCO-medewerkers en GGD-medewerkers aangescherpt. Dit is aangescherpt naar aanleiding van de datadiefstal.

Wanneer gaan jullie een ander systeem invoeren voor het bron- en contactonderzoek?
GGD Contact is het door het ministerie van het ministerie van VWS, GGD GHOR Nederland en alle GGD'en aangewezen als vervangend systeem voor HPZone Lite en is bij alle GGD'en en landelijke partners geïmplementeerd. GGD Contact voldoet aan alle moderne eisen op het gebied van privacy- en informatiebeveiliging. GGD Contact is ontwikkeld door het Ministerie van VWS en wordt gebruikt voor het bron- en contactonderzoek (BCO) door de GGD'en en de landelijke partners. Bij GGD Contact, het door het ministerie van VWS, GGD GHOR Nederland en alle GGD'en aangewezen vervangend systeem voor HPZone Lite, zijn informatiebeveiliging en privacy integrale onderdelen geweest van de ontwikkeling en implementatie.

Persoonlijke gegevens

Welke informatie van mensen staat in CoronIT en HP Zone?
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 HP Zone staan naam, adres, woonplaats, telefoonnummer, geslacht, geboortedatum en BSN van een persoon. Verder wordt in HP Zone ook de informatie uit de bron- en contactonderzoek gesprekken vastgelegd. Dit is onder andere: noodzakelijke medische gegevens (bijvoorbeeld 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 HP Zone, deze zijn terug te vinden in de privacyverklaring van bron- en contactonderzoek in het kader van COVID-19.

Waarom zijn persoonlijke gegevens zoals BSN, geboortedatum, telefoonnummer en e-mailadres nodig voor het maken van een test- of vaccinatieafspraak?
Volgens de Wet op de geneeskundige behandelovereenkomst (WGBO) zijn we verplicht om een geboortedatum uit te vragen en vast te leggen bij een te testen of te vaccineren persoon. Zo weten we zeker dat wij te maken hebben met de juiste persoon. Het telefoonnummer is nodig om contact op te kunnen nemen in het geval een test- of vaccinatieafspraak niet door kan gaan. Bijvoorbeeld bij slechte weersomstandigheden of als het vaccineren ineens wordt stilgelegd zoals bij AstraZeneca tijdelijk aan de orde was. Het e-mailadres is nodig om per e-mail een test- of vaccinatieafspraak te kunnen bevestigen. En, wenselijk op het moment dat er onverhoopt een verkeerd telefoonnummer is geregistreerd om iemand te kunnen bereiken.

De wet Aanvullende bepalingen verwerking persoonsgegevens in de zorg bepaalt dat wij het BSN-nummer moeten uitvragen. De GGD'en zijn wettelijk verplicht om het **BSN-nummer** te verwerken. Indien burger deze gegevens niet wil geven, vindt er geen vaccinatie plaats.

Welke gegevens van een persoon kunnen de medewerkers inzien?
Dat hangt van de rol van de gebruiker af. De gebruiker ziet alleen die gegevens die hij of zij op dat moment voor zijn werk nodig heeft. Voor mensen die werken bij het callcenter dat testafspraken maakt zijn bijvoorbeeld de gezondheidsverklaringen die voor vaccinaties worden ingevuld niet zichtbaar. Registratie van bijwerkingen is alleen toegankelijk voor mensen met medische autorisatie.

Staan de gegevens van alle Nederlanders in CoronIT en HP Zone?
Nee, in CoronIT staan alleen de gegevens van personen die een test- of vaccinatie afspraak bij een GGD hebben gemaakt. In HP Zone staan alleen de gegevens van de personen die een positieve COVID-19 test hebben ontvangen en van mensen die als huisgenoot of als nauw contact uit bron- en contactonderzoek kwamen.

Hoe lang blijven mijn persoonsgegevens bewaard?
Wij houden ons aan de wettelijke termijnen die hiervoor gelden. Wij verwijderen uw persoonsgegevens als deze niet langer noodzakelijk zijn. Voor HPzoneLite geldt een maximale bewaartermijn van 5 jaar, voor data in CoronIT 20 jaar. We bewaren persoonsgegevens in ieder geval voor de gehele duur van de pandemie.