Bijlage: Toelichting CBS bij brief RIVM aan DPG'en over samenwerking CBS tbv COVID-19 bestrijding

Het CBS biedt aan een gezamenlijk onderzoek te doen met RIVM op basis van COVID-19 meldingsdata en SARS-CoV-2 testdata. Doel van dit onderzoek is om met de combinatie van testdata- en meldingsdata én de data die het CBS in huis heeft nieuwe maatschappelijke patronen te ontdekken en te herkennen die kunnen bijdragen aan het bestrijden van verdere verspreiding van het virus.

Het CBS beschikt over een veelheid van data over vrijwel alle personen in Nederland. Via de GGD'en zijn gegevens bekend van mensen die een positieve test-uitslag hebben (en daarmee onder de wettelijke meldingsplicht vallen). Via het landelijke registratiesysteem CoronIT zijn ook gegevens beschikbaar van personen getest in de GGD testfaciliteiten; zowel van degenen met een positieve als met een negatieve testuitslag. De combinatie van deze corona databronnen aan de CBS data maakt aanvullend onderzoek mogelijk dat op de corona test- en meldingsdata alleen niet mogelijk is. Voor dergelijk onderzoek is het noodzakelijk deze data bij het CBS ter beschikking te krijgen.

Hieronder volgt eerst de juridische context voor de koppeling van de GGD COVID-19 meldingsgegevens aan databronnen beschikbaar bij CBS. Vervolgens een aantal additionele veiligheidsmaatregelen, zowel technisch als inhoudelijk, die samenhangen met het doen van een gezamenlijk onderzoek. Daarna wordt een aantal mogelijke onderzoeksonderwerpen geschetst. Welk onderzoek daadwerkelijk wordt opgepakt is nog afhankelijk van onderlinge afstemming tussen RIVM, GGD'en en CBS.

Juridische context

Naar aanleiding van de vraag van RIVM en GGD GHOR over de rechtmatigheid van de verzochte verstrekking van persoonsgegevens waaronder BSN's (hierna: de "Persoonsgegevens") aan het CBS is deze vraag voorgelegd aan de CBS juristen. Op basis van onderstaande toelichting/analyse komt CBS tot de volgende conclusie: de verzochte verstrekking van Persoonsgegevens aan het CBS voldoet aan de relevante AVG/UAVG-vereisten en is daarmee rechtmatig.

Voor het verstrekken van de persoonsgegevens aan het CBS door de GGD moet in het kader van AVG en andere toepasselijke wetgeving voldaan worden aan twee voorwaarden:

1. **Doelbinding**

   Het doelbindingsvereiste zoals is opgenomen in artikel 5.1.a. AVG: "Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding")".

   Op grond van de CBS-wet (art. 37 lid 1) mag CBS de van GGD te ontvangen Persoonsgegevens uitsluitend gebruiken voor statistische doeleinden. De verenigbaarheid tussen het oorspronkelijke verzameldoel van GGD en het verdere (statistische) verwerkingsdoel van het CBS staan dus op grond van de laatste volzin van art. 5.1.a vast.

   Conclusie: Omdat onder verwerking ook verstrekking aan derden valt is de verdere verwerking voor statistiek altijd verenigbaar.

2. Juridische grondslag

De GGD heeft een juridische grondslag nodig om de gegevens verder te mogen verwerken en dus te kunnen verstrekken aan het CBS (AVG). Het CBS heeft op zijn beurt een grondslag nodig om de gegevens te mogen verwerken en verstrekken aan het RIVM (CBS-wet en AVG).

Het CBS gaat er vanuit dat de verkrijging/verzameling door de GGD van de betreffende Persoonsgegevens (incl. BSN) gebaseerd is op een juridische grondslag dus rechtmatig was/is en dat de GGD (als verwerkingsverantwoordelijke voor de verzameling van deze Persoonsgegevens) hiervoor dus onder meer de vereiste (verwerkings)grondslag als bedoeld in artikel 6 lid 1 AVG beschikbaar heeft.

De AVG of de UAVG bevatten geen enkel aanknopingspunt voor de opvatting dat de hiervoor bedoelde uitzondering op het doelbindingsvereiste niet zou gelden ingeval van 'bijzondere persoonsgegevens' of (nog strenger beschermde) nationale identificatienummers (zoals BSN's). Daarom is CBS van mening dat ook als een BSN eenmaal rechtmatig is verzameld (en dus o.a. daarvoor een grondslag als bedoeld in artikel 6 lid 1 AVG beschikbaar is) het vervolgens ook rechtmatig met CBS gedeeld kan worden ten behoeve van statistisch/wetenschappelijk onderzoek (omdat dit doeleinde altijd verenigbaar is met het oorspronkelijke verzameldoel).

Voor BSN's gelden echter bijzondere (aanvullende) vereisten, zodat het enkel hebben van een verwerkingsgrondslag als bedoeld in art. 6 lid 1 AVG onvoldoende is. Van belang is met name dat op grond van artikel 87 AVG jo. 46 UAVG (kort gezegd) een wettelijke grondslag moet bestaan voor de verwerking van BSN's. Voor levering van BSN's aan CBS is deze wettelijke grondslag opgenomen in artikel 34 van de Wet CBS (http://wetten.overheid.nl/BWBR0015926/2018-07-28). Verder mag het CBS op basis van artikel 35 CBS Wet ten behoeve van statistische doeleinden bijzondere categorieën van persoonsgegevens ontvangen zoals bedoeld in paragraaf 3.1 en 3.2 van de Uitvoeringswet Algemene verordening gegevensbescherming.

Conclusie: Op grond van het voorgaande is het CBS van mening dat voor zover GGD de Persoonsgegevens (inclusief BSN's) rechtmatig heeft verzameld het ook rechtmatig is om die Persoonsgegevens met CBS te delen ten behoeve van statistisch onderzoek.

Na ontvangst van de Persoonsgegevens zal het CBS 'verwerkingsverantwoordelijke' zijn voor alle verdere 'verwerkingen' die plaatsvinden. CBS doet deze verwerkingen in het kader van zijn wettelijke taak als bedoeld in artikel 3 Wet CBS, zodat het CBS voor deze verdere verwerkingen de verwerkingsgrondslag uit artikel 6 lid 1 sub c AVG kan gebruiken.

De wetsgeschiedenis van de UAVG onderschrijft de hiervoor gegeven analyse (Kamerstukken II 2017/18, nr. 3 (MvT), p. 37-39):
"Verdere verwerking ziet in de verordening op verwerkingen van persoonsgegevens voor een ander doel dan waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Dit kan verwerking door één en dezelfde verwerkingsverantwoordelijke zijn, maar kan ook de verstrekking van gegevens aan een andere verwerkingsverantwoordelijke inhouden. De verwerkingsverantwoordelijke die de gegevens ontvangt, zal voor de verwerking van de ontvangen gegevens uiteraard een zelfstandige rechtsgrondslag nodig hebben als bedoeld in artikel 6, eerste lid, van de verordening bijvoorbeeld dat de verwerking noodzakelijk is voor de uitoefening van de taak van algemeen belang.
[...]
Als kan worden vastgesteld dat er sprake is van een verenigbaar doel, is voor de verdere verwerking geen andere afzonderlijke rechtsgrond vereist dan die op grond waarvan de

verzameling van de persoonsgegevens werd toegestaan. De Unierechtelijke of lidstatelijke bepaling die als rechtsgrond voor de verwerking van persoonsgegevens dient, kan ook dienen als rechtsgrond voor de verdere verwerking voor een verenigbaar doel. Dit geldt voor alle verwerkingsverantwoordelijken, derhalve ook voor overheidsinstanties. Er is geen reden om aan te nemen dat in geval van overheidsinstanties er altijd een specifieke grondslag moet zijn voor verdere verwerking, als het gaat om een doel dat verenigbaar is met het oorspronkelijke doel. Voorts is van belang dat uit artikel 5, eerste lid, onderdeel b, van de verordening voortvloeit dat verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden niet als onverenigbaar met de oorspronkelijke doeleinden worden beschouwd. Op grond van de verordening blijft derhalve ook verdere verwerking voor voornoemde doeleinden onverminderd mogelijk. Voorwaarde voor de verdere verwerking voor die doeleinden is wel dat de verantwoordelijke voorziet in passende waarborgen voor de bescherming van de persoonsgegevens van de betrokkenen. Bij de mogelijke voorzieningen die de verantwoordelijke in dit kader kan treffen, kan bijvoorbeeld worden gedacht aan het pseudonimiseren van de desbetreffende persoonsgegevens."

Maatregelen bij het doen van gezamenlijk onderzoek

Het samenstellen van veilige informatie (in de vorm van statistieken) op basis van zeer privacygevoelige microdata is de kerntaak van het CBS. Het CBS verzamelt gegevens van natuurlijke personen, bedrijven en instellingen. Verreweg de meeste gegevens zijn afkomstig uit administraties en registers die in gebruik zijn bij de overheid. Het CBS ontvangt het merendeel van deze administraties en registers integraal en met regelmaat.

Direct identificerende persoonskenmerken worden zo snel als mogelijk na ontvangst vervangen door een pseudosleutel. Met deze gepseudonimiseerde gegevens doet het CBS vervolgens statistisch onderzoek.

Het CBS publiceert alleen statistische informatie waarin natuurlijke personen niet herkenbaar of herleidbaar zijn. Ook hebben we maatregelen genomen tegen diefstal, verlies of misbruik van persoonsgegevens. Het CBS levert nooit herkenbare gegevens aan derden, ook niet aan andere overheidsinstellingen. Wel kunnen (wetenschappelijke) instellingen onder strenge voorwaarden toegang krijgen tot gepseudonimiseerde gegevens op persoons- of bedrijfsniveau (zie verderop).

Het CBS is gehouden aan deze strikte bescherming van de privacy via de CBS-wet, de Europese Code of Conduct voor statistiekbureaus en de AVG. Het CBS voldoet aan de hoogste eisen m.b.t. gegevensbescherming. Dit wordt jaarlijks getoetst door een externe organisatie en resulteert in een privacy-proof verklaring. Daarmee voldoet het CBS aantoonbaar aan de verplichtingen van de AVG (de verantwoordingsplicht).

Bij beschikbaarstelling van data, specifiek voor een gezamenlijk project tussen het CBS en een derde partij (in dit geval RIVM en GGD'en) wordt de data slechts gebruikt voor het project in kwestie. De data wordt niet gebruikt voor andere doeleinden, tenzij na uitdrukkelijke toestemming van de bronhouder(s).

Bij de uitvoering van een gezamenlijk project zijn alle partijen verantwoordelijk voor de juistheid van de rapportages en de daarbij horende inzichten en conclusies. Deze zijn verwoord in een gezamenlijke rapportage en een gezamenlijke publicatie. Bij wetenschappelijke publicaties en openbare statistieken heeft geen van de betrokken partijen het recht om met resultaten naar buiten te komen zonder nadrukkelijke toestemming van de andere partijen. Deze afspraken worden vastgelegd in een overeenkomst tussen CBS, RIVM, en GGD'en.

Het is niet gebruikelijk om met gegevens naar buiten te treden wanneer een statistiek/statistisch onderzoek nog niet is afgesloten, beoordeeld en gepubliceerd. Dit is vast uitgangspunt van wetenschappelijke integriteit van zowel CBS, als RIVM, als de GGD'en. Het is echter voorgekomen dat het RIVM bij de uitoefening van zijn wettelijke adviestaak als gevolg van dringende opdracht tot risicobeoordeling en/of advisering aan het bestuurlijk niveau, gebruik moet maken van nog niet gepubliceerd statistisch inzicht. In die situatie vermeldt het RIVM nadrukkelijk dat gepresenteerde gegevens voorlopig van aard en nog niet gepubliceerd zijn. En informeert het RIVM de partners tevoren over deze vroegtijdige uiting. Deze uitzonderingssituatie geldt uitsluitend wegens de unieke situatie van de COVID-19 epidemie voor de gegevens die voortvloeien uit dit project en die reeds van voldoende kwaliteit zijn om openbaar te maken. Indien de informatie in de bovengenoemde situatie nog niet openbaar is gemaakt, zal dit alsnog binnen twee weken geschieden. Indien sprake is van enig risico dan is dat voor rekening van het RIVM.

Toegang tot gekoppelde data door GGD voor eigen data

Het is voor organisaties die statistisch wetenschappelijk onderzoek doen mogelijk om toegang te krijgen tot de CBS-data. Hiervoor is een machtiging nodig van de DG van het CBS. Voor een aantal GGD'en geldt dat (de onderzoeksafdeling van de betreffende GGD) deze toestemming al heeft. RIVM beschikt eveneens over een dergelijke machtiging. Overige GGD'en die onderzoek willen doen op de microdata van het CBS, in combinatie met de eigen gegevens, kunnen een dergelijke machtiging aanvragen. Informatie hierover is te vinden op de website van het CBS.

Gegevensuitwisseling: praktische details

Het CBS ontvangt vele honderden bestanden, registers en administraties en kent meerdere technieken en kanalen daarvoor. Alle technieken zijn veilig en voor dit doel geschikt en gecertificeerd. De uiteindelijke keuze voor een bepaalde techniek vindt plaats in overleg met alle betrokken partijen. Daarbij wordt onder andere gekeken naar de privacygevoeligheid van de gegevens, de omvang en de frequentie van de leveringen. Hieronder volgt een overzicht van mogelijke technieken.

Upload HTTPS

Een van de technieken waarmee u digitale databestanden aan het CBS kunt leveren, is Upload HTTPS. HTTPS staat voor HyperText Transfer Protocol Secure en is een door middel van transportversleuteling beveiligde internetverbinding. Met behulp van deze techniek bent u als dataleverancier (berichtgever) in staat databestanden beveiligd via het internet aan het CBS te leveren. Inloggegevens worden u per e-mail of brief verstrekt. Dit kanaal is veilig en laagdrempelig. U heeft alleen een moderne browser nodig om hier gebruik van te kunnen maken. Deze techniek wordt voornamelijk gebruikt voor data die handmatig aan het CBS worden aangeleverd.

Upload SFTP

Een andere techniek waarmee u digitale databestanden aan het CBS kunt leveren, is Upload SFTP. SFTP staat voor Secure File Transfer Protocol. Er zijn twee manieren om een connectie te maken met de SSH-server van het CBS. De eerste mogelijkheid is via een user/passwordcombinatie. De user/passwordcombinatie krijgt u als dataleverancier van het CBS per brief of e-mail. De andere mogelijkheid is via een public key. Een public key is een van de twee sleutels die gebruikt worden voor asymmetrische cryptografie. Bij deze wijze van informatieversleuteling zijn er twee verschillende sleutels die bij elkaar horen: één voor vercijferen en één voor ontcijferen van informatie. U als dataleverancier (berichtgever) stuurt de public key (als eigenaar) naar het CBS. Nadat de verbinding tot stand is gekomen, hebt u toegang tot een remote folder (externe map) op de SSH-server van het CBS, waar databestanden bedoeld voor een bepaalde statistiek naar toe gekopieerd kunnen worden. De bestanden in deze remote folder kunnen niet geopend, verwijderd

of teruggehaald worden. Dat is beveiligd. Op regelmatige tijden wordt deze folder door het CBS geleegd en worden de databestanden verwerkt. Deze techniek is voornamelijk bedoeld om volledig geautomatiseerd digitale databestanden beveiligd via het internet aan het CBS te leveren.

Digipoort (Logius)

Digitaal informatie uitwisselen met collega-overheidsorganisaties en bedrijven is eenvoudig en efficiënt mogelijk via Digipoort, Digikoppeling, Diginetwerk, Digimelding en de Stelselcatalogus. Via Digipoort kunnen overheidsorganisaties en bedrijven snel en efficiënt digitaal informatie uitwisselen. Digikoppeling maakt grootschalig elektronisch berichtenverkeer tussen overheidsorganisaties mogelijk. Diginetwerk maakt het mogelijk dat overheden binnen één besloten virtueel overheidsnetwerk veilig gegevens kunnen uitwisselen. Digimelding is één centraal punt voor melden van onjuistheden in basisregistraties. De Stelselcatalogus beschrijft de structuur van het stelsel van basisregistraties en ook de definities van soorten objecten, gegevens en berichten.

Bij digipoort kan het gaan om berichten die nog een verdere bewerking nodig hebben voordat ze verwerkt kunnen worden of complexere berichtenstromen waar meerdere (overheids)partijen bij zijn betrokken. Digipoort maakt gebruik van een besloten netwerk en kan alleen worden gebruikt wanneer u als dataleverancier ook bent aangesloten op Digipoort.

RINIS

RINIS staat voor Routerings Instituut (inter)Nationale Informatiestromen. Op dit moment zijn elf Nederlandse uitvoerders van publieke taken (sectoren) bij RINIS aangesloten:

- Belastingdienst
- Centraal Administratie Kantoor (CAK)
- Centraal Bureau voor de Statistiek (CBS)
- Dienst Uitvoering Onderwijs (DUO)
- Ministerie van Justitie
- Dienst Justitiële Inrichtingen (DJI)
- Landelijk Bureau Inning Onderhoudsbijdragen (LBIO)
- Raden voor Rechtsbijstand
- Stichting Inlichtingenbureau, het sectorloket van gemeentelijke sociale diensten
- Stichting Netwerk Gerechtsdeurwaarders (SNG)
- Sociale Verzekeringsbank (SVB)
- Uitvoeringsinstituut Werknemersverzekeringen (UWV)
- Zorgverzekeraars Nederland (ZN)

RINIS is een onafhankelijke stichting zonder winstoogmerk en wordt bestuurd door een Raad van Toezicht. RINIS is een berichtendienst voor volledig geautomatiseerde gegevensuitwisselingen tussen de aangesloten sectoren. RINIS richt deze uitwisselingen in en beheert ze. RINIS sluit sectoren aan op het eigen netwerk (RINIS.net) en zorgt voor de aanschaf van de juiste hard- en software. RINIS maakt gebruik van een besloten netwerk en kan alleen worden gebruikt wanneer u als dataleverancier ook bent aangesloten op RINIS.