

Het CBS vraagt om beschikbaarstelling van identificerende gegevens (BSN of een combinatie van geslacht, geboortedatum en adres) over mensen die zijn getest op Corona. Positieve testuitslagen zijn bijzonder waardevol, negatieve testuitslagen echter eveneens. Het CBS vraagt bovendien om nieuwe resultaten met regelmaat te leveren zodat trends in de tijd kunnen worden waargenomen. Voornamelijk gaat het hier om een tijdelijke levering, totdat de Corona-crisis bezworen is. Hier is op dit moment (nog) geen datum op vast te leggen. We stellen daarom 1 oktober als einddatum voor.

Hieronder zal ik achtereenvolgens in gaan op het doel van de gegevenslevering, de bescherming van de privacy, de beschikbaarstelling van data voor wetenschappelijk/statistisch onderzoek, extra plausibiliteitschecks en de juridische context.

Doel van de gegevenslevering.

Het CBS heeft vragen gekregen van onder andere de NCTV, diverse ministeries, de VNG en diverse gemeenten om ondersteunende informatie te leveren voor het beleid ten aanzien van de bestrijding van de Corona crisis, dan wel te ondersteuning van mitigerend beleid om de gevolgen van de Coronacrisis te verzachten.

Om dit (nog) beter te kunnen doen is het beschikken over Coronatest-data belangrijk. Op de eerste plaats kunnen we hiermee vele honderden achtergrondkenmerken van personen koppelen aan de patiënten. We kunnen zo zien of er onder de patiënten een oververtegenwoordiging is in bepaalde beroepsgroepen of bijvoorbeeld bepaalde migratieachtergronden. We kunnen patronen ontdekken die te maken hebben met familierelaties, we kunnen hypothesen rond de verspreiding ('Groningse studenten', 'wintersporters', 'carnavalliezers') testen en eventueel bevestigen of ontkrachten. We kunnen een koppeling maken met medicijngebruik en medische voorgeschiedenis. En uiteraard nog veel meer.

We kunnen aan de hand van die uitkomsten conclusies trekken ten aanzien van de omvang en eventueel geografische verspreiding van een potentiële risicogroep.

Op de tweede plaats kunnen we deze data beschikbaar maken voor wetenschappelijk onderzoek. Het CBS beschikt over een geheel veilige en privacy protected omgeving waar wetenschappelijk statistische onderzoek kan worden gedaan. Er zijn al verzoeken binnengekomen vanuit LUMC, Groningen, TNO, AHTI, universiteit van Maastricht en UvA. Er is in Nederland veel wetenschappelijk onderzoek gedaan naar bijvoorbeeld verspreiding van AIDS, kennis en ervaring die nuttig ingezet kan worden bij het bestrijden van de Corona crisis. Daarnaast is in een aantal wetenschappelijke databases informatie beschikbaar over specifieke medische voorgeschiedenis en genetische informatie. Nederland is wereldwijd een van de zeer weinige landen waar de mogelijkheid bestaat deze data te koppelen aan Coronatest-data. Deze koppeling kan behulpzaam zijn bij ontwikkeling van vaccins en medicijnen.

Ten aanzien van bescherming van de privacy

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 pseudoniem. 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).

Beschikbaarstelling van microdata voor wetenschappelijke doeleinden

Het CBS beschikt als een van de weinige statistiekbureaus in de wereld over een infrastructuur waarmee de microdata van het statistiekbureau in gepseudonimiseerde vorm beschikbaar kan worden gesteld voor wetenschappelijk/statistisch onderzoek. Dit is aan zeer strenge voorwaarden verbonden en omkleedt met tal van veiligheidseisen. Het gaat te ver om alle veiligheidseisen hier te noemen, meer informatie is te vinden op de website van het CBS: www.cbs.nl/microdata.

Voor deze toegang dienen de gebruikers in te loggen op de systemen van het CBS. Van daaruit is het niet mogelijk data te exporteren. Dit is slechts mogelijk na een controle door het CBS op onthulling. Bij deze controle vergewissen wij ons er van dat de onderzoeksresultaten statistiek zijn, dat wil zeggen dat er geen informatie over een individueel persoon, huishouden of organisatie/bedrijf uit af te leiden is.

Bij gebruik voor wetenschappelijke doelen wijzen wij er op dat naast technische en juridische eisen vanuit het CBS alleen wordt samengewerkt met wetenschappelijke initiatieven die zelf ook voldoen aan hoge eisen ten aanzien van bescherming van de privacy.

Ten aanzien van de plausibiliteit van de onderzoeksresultaten

Analyse van de gegevens is ingewikkeld omdat testen niet at random zijn gedaan. Door rekening te houden met de kans op testen én gebruik te maken van de rijke achtergrondinformatie van het CBS kunnen waarschijnlijk toch heel bruikbare analyses gedaan worden. Afgesproken is dat RIVM meekijkt met de resultaten voordat die gepubliceerd worden als extra plausibiliteitscheck.

Het CBS wijst er op dat het CBS een strikt onafhankelijke positie heeft. Het CBS stelt een plausibiliteitscheck door het RIVM ten zeerste op prijs en zal de uitkomsten daarvan meenemen als een zeer zwaarwegend advies meenemen in het besluit om al dan niet de resultaten te publiceren.

Om een goede afweging te maken van de over- of ondervertegenwoordiging van geteste personen in een populatie is het zeer behulpzaam om óók te beschikken over identificerende gegevens van personen die met negatieve testresultaten.

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 heb ik deze vraag voorgelegd aan onze 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 dus rechtmatig.

Voor het verstrekken van de persoonsgegevens aan het CBS door de GGD moet 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")".

GGD heeft de Persoonsgegevens verzameld ten behoeve van een bepaald doel (welk doel dat is, is voor de analyse verder niet relevant). Het doelbindingsvereiste zoals opgenomen in artikel 5 lid 1 sub b AVG brengt met zich dat het dan niet toegestaan is deze Persoonsgegevens verder te 'verwerken' voor een doel dat niet verenigbaar is met het oorspronkelijke verzameldoel. Daarbij geldt dat volgens de definitie van 'verwerking' (art. 4 sub 2 AVG) ook het verstrekken van Persoonsgegevens aan een derde (zoals het CBS) kwalificeert als een 'verwerking'. In principe is het gelet op artikel 5 lid 1 sub b AVG hierdoor enkel toegestaan om de voor een bepaald doel door GGD verzamelde Persoonsgegevens met het CBS te delen voor doeleinden die verenigbaar zijn met het oorspronkelijke verzameldoel van GGD.

De vraag is dus of de doeleinden waarvoor GGD de Persoonsgegevens aan het CBS zou verstrekken verenigbaar zijn met de oorspronkelijke verzameldoelen van GGD. In dat verband is relevant dat artikel 5 lid 1 sub b AVG bepaalt dat verdere 'verwerking' (waaronder blijkens de AVG-definitie van 'verwerking' dus ook valt het verstrekken aan een derde zoals het CBS) ten behoeve van 'wetenschappelijk of historisch onderzoek of statistische doeleinden' per definitie een verenigbaar doeleinde is (artikel 89 lid 1 AVG). Dit geldt onafhankelijk van de vraag wat het oorspronkelijke verzameldoel was en dus maakt het voor de analyse niet uit wat de verzameldoelen van GGD waren.

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 vast.

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

2. De GGD heeft een juridische grondslag nodig om de gegevens verder te mogen verwerken en dus te kunnen verstrekken aan het CBS (AVG en evt andere toepasselijke wetgeving?). 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 statistisch 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.”