AUTORITEIT
PERSOONSGEGEVENS

Rapport naar aanleiding van onderzoek gegevensverwerking SBG

Definitief rapport

Inhoudsopgave

Samenvatting

Inleiding

Al enige tijd is er discussie over het gebruik van *Routine Outcome Monitoring* [1] (ROM) als meetinstrument voor de kwaliteit van zorg in de Geestelijke Gezondheidszorg (GGZ) en of deze gegevens zijn te kwalificeren als persoonsgegevens in de zin van voorheen de Wet Bescherming Persoonsgegevens (Wbp) en nu de Algemene Verordening Gegevensbescherming (AVG).

In dat verband heeft de Autoriteit Persoonsgegevens (AP) een handhavingsverzoek[2] ontvangen waarin is verzocht om jegens Stichting Benchmark GGZ (SBG) handhavend op te treden. SBG is opgericht om met ROM-data de kwaliteit van zorg in de GGZ inzichtelijk en meetbaar te maken onder meer door middel van benchmarking, zodat zorgaanbieders hiervan konden leren en de kwaliteit van zorg konden verbeteren.

Volgens verzoekster zijn voornoemde ROM-data persoonsgegevens en, nu SBG ROM-data en daarmee volgens verzoekster persoonsgegevens verwerkt(e) zonder wettelijke grondslag (want zonder haar toestemming), heeft zij de AP verzocht om de verzameling en verwerking van gegevens door SBG te laten staken, de gehele databank te laten verwijderen en toe te zien op hernieuwde wederrechtelijke vulling.

Onderzoek

De AP heeft naar aanleiding van het handhavingsverzoek onderzoek gedaan. Het onderzoek heeft zich met name gericht op de vraag of SBG persoonsgegevens verwerkt. Het antwoord op deze vraag bepaalt immers het verdere verloop van het onderzoek. Voor de beantwoording van deze vraag, moest inzichtelijk en begrepen worden welke data bij SBG aangeleverd werden. Daartoe was het van belang alle stappen van het gegevens-aanleverproces van patiënt tot en met de verwerking van de betreffende gegevens door SBG en de in dat verband betrokken partijen en gemaakte afspraken te betrekken en te toetsen aan de relevante wet- en regelgeving.

Tijdens het onderzoek werd bekend dat SBG haar activiteiten zou gaan staken en een groot deel van haar activiteiten en de door haar verzamelde en bewerkte gegevens zou overdragen aan Alliantie Kwaliteit in de geestelijke gezondheidszorg (Akwa). Dit was voor de AP aanleiding ook onderzoek te verrichten naar de gegevens die door SBG nog zouden worden bewaard en aan Akwa zouden worden overgedragen.

Conclusies

De AP komt tot de conclusie dat de data die SBG (via ZorgTTP) van zorgaanbieders heeft ontvangen een verwerking is van persoonsgegevens over de gezondheid in de zin van artikel 4, onderdeel 1 en 15, AVG. De AP concludeert daarnaast dat SBG zich niet kan beroepen op één van de wettelijke uitzonderingsgronden die het verbod om gegevens over gezondheid te verwerken zou kunnen opheffen. Dit heeft tot gevolg dat het voor SBG op grond van artikel 9, eerste lid, AVG verboden is om de dataset met daarin persoonsgegevens over de gezondheid te verwerken.

[1] Routine outcome monitoring (afgekort als 'ROM') is de methodiek in de geestelijke gezondheidszorg waarbij regelmatig metingen gedaan worden van de toestand van de cliënten met het oog op evaluatie en eventueel bijsturing van de behandeling. Dit gaat middels het invullen van vragenlijsten door de patiënt.
[2] In AVG terminologie een klacht genaamd.

1. Aanleiding en verloop van het onderzoek

1.1 Aanleiding

Aanleiding voor het onderzoek vormt een handhavingsverzoek van 24 maart 2017 waarin de AP is verzocht om handhavend op te treden jegens SBG vanwege het - zonder toestemming - verzamelen en verwerken van (medische en bijzondere) persoonsgegevens door SBG.

In het handhavingsverzoek wordt verzocht om het verzamelen en verwerken van (medische en bijzondere) persoonsgegevens in de databank van SBG zo spoedig mogelijk op te schorten en toe te zien op de vernietiging per direct van de gegevens in de SBG-databank. Ook dient toezicht plaats te vinden op hernieuwde wederrechtelijke vulling van de databank.

1.2 Doel onderzoek

Het onderzoek heeft als doel vast te stellen of SBG persoonsgegevens verwerkt en of deze verwerking in overeenstemming is met de AVG. Het onderzoek richt zich daarbij op de verwerking die bestaat uit de ontvangst en bewaring van de gegevens door SBG. De AP heeft onderzocht of SBG aldus persoonsgegevens heeft ontvangen en of deze persoonsgegevens betrekking hebben op de gezondheid van betrokkenen. Vervolgens heeft de AP onderzocht of SBG zich kan beroepen op een wettelijke uitzonderingsgrond op het verbod van verwerking van persoonsgegevens betreffende de gezondheid. De AP heeft ten slotte onderzocht of de dataset die SBG aan Akwa heeft overgedragen persoonsgegevens zijn.

1.3 Verloop van het onderzoek[3]

De AP heeft SBG op de hoogte gesteld van het handhavingsverzoek. SBG heeft op 24 april 2017 op het handhavingsverzoek haar zienswijze gegeven en desgevraagd bij brief van 25 augustus 2017 nadere informatie aan de AP verstrekt.

De gegevensverwerking door SBG, zoals aan de orde in onderhavig handhavingsverzoek, is eerder onderwerp geweest van een civielrechtelijke procedure. Op 2 augustus 2017 is een vonnis in kort geding gewezen[4] waarbij de rechter oordeelde dat niet voldoende aannemelijk is geworden dat sprake is van de verwerking van persoonsgegevens in de zin van de Richtlijn[5] en de Wbp.

Op 11 juli 2018 heeft de AP een gesprek gevoerd met SBG waarin door SBG is toegelicht dat in de nabije toekomst alleen nog data zullen worden verwerkt met toestemming van de patiënt. Die verwerking zou plaats moeten vinden door een onafhankelijk kwaliteitsinstituut.

Op 3 december 2018 heeft de AP, naar aanleiding van een ingebrekestelling van verzoekster, beslist op het handhavingsverzoek. Het handhavingsverzoek is bij dit besluit afgewezen omdat het onderzoek op dat

[3] Hierna volgt een beknopt verloop van het onderzoek. Als bijlage 1 bij dit rapport is het uitgebreidere procesverloop gevoegd.
[4] ECLI:NL:RBMNE:2017:4011
[5] Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens

moment nog niet was afgerond en er derhalve voor de AP geen mogelijkheid bestond om handhavend op te treden. Verzoekster heeft op 10 januari 2019 pro forma bezwaar gemaakt tegen voormeld besluit.

De AP is door SBG op 27 november 2018 per brief geïnformeerd dat SBG zal ophouden te bestaan en dat Akwa de rol van SBG zal overnemen. Naar aanleiding daarvan hebben Akwa en SBG desgevraagd op 16 januari en 6 februari 2019 nog aanvullende informatie aan de AP gegeven.

2. Het handhavingsverzoek

Het handhavingsverzoek bevat een aantal gronden op basis waarvan de AP verzocht wordt handhavend op te treden. Deze worden hieronder verkort weergegeven.

Gronden handhavingsverzoek
Verzoekster stelt dat SBG haar medische gegevens verwerkt zonder haar toestemming. Deze gegevens zijn volgens verzoekster aan te merken als (medische en bijzondere) persoonsgegevens. Daarmee is volgens verzoekster sprake van een onrechtmatige verwerking van haar persoonsgegevens. Ze wijst daarbij op de herleidbaarheid van de desbetreffende gegevens tot individuen, ook voor zover het gaat om gepseudominiseerde gegevens. De minister heeft volgens verzoekster dit standpunt destijds onderschreven.

Daarnaast maakt verzoekster een vergelijking tussen de databank van SBG en het DBC-informatiesysteem (DIS) van de Nederlandse Zorgautoriteit, waarvan de AP heeft geoordeeld dat de daarin vervatte data persoonsgegevens zijn. Omdat bij het DIS[6] het CBS beschikt over de mogelijkheid om gegevens te ontsleutelen, vraagt ze zich af of het CBS daartoe ook de mogelijkheid heeft bij ZorgTTP. Verzoekster wijst ook op een mogelijke koppeling van de SBG-meetgegevens aan een DBC-traject of via een koppeling met DIS en Vektis waardoor volgens verzoekster (indirect) identificatie mogelijk is.

Ook voert verzoekster aan dat er onduidelijkheid is of de databank van SBG wel veilig is en gecertificeerd is conform beveiligingsnormen voor informatiesystemen en betwijfelt ze - gelet op de financieringsconstructie van SBG en de participatie van zorgverzekeraars in SBG - evenzeer of SBG wel een Trusted Third Party (TTP) is.

Onder verwijzing naar de aansluitvoorwaarden SBG 20161001 geeft verzoekster aan dat de BRaM-rapportages (Benchmark Rapportage Module) kunnen worden gekoppeld aan databases en systemen van andere organisaties. In het bijzonder wijst zij op de connecties van VECOZO en Vektis met zorgverzekeraars en andere organisaties. Hierdoor zouden (medische/bijzondere) persoonsgegevens kunnen worden verwerkt.

Verzoek
Volgens verzoekster betekent het vorenstaande dat sprake is van schending van de Wbp en de Wet op de geneeskundige behandelingsovereenkomst (Wgbo). Daarom verzoekt zij de AP het verzamelen en verwerken van (medische en bijzondere) persoonsgegevens in de databank van SBG, zo spoedig mogelijk op te schorten en toe te zien op de vernietiging per direct van de gegevens in de SBG-databank. Ook dient volgens verzoekster toezicht plaats te vinden op hernieuwde wederrechtelijke vulling van de databank.

[6] DIS staat voor Diagnose Informatie Systeem. Informatie over diagnoses van patiënten in de ziekenhuiszorg, geestelijke gezondheidszorg en forensische zorg komt terecht in DIS en wordt beheerd door de Nederlandse Zorgautoriteit. Zie ook: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-nza-mag-diagnosegegevens-uit-dis-beperkt-verstrekken

3. Feiten

Het handhavingsverzoek werpt allereerst de vraag op of SBG over persoonsgegevens beschikt en verwerkt c.q. verwerkte in de zin van de Wbp en de AVG. Voor de beantwoording van die vraag is het van belang om allereerst de relevante informatiestromen inzichtelijk te maken; wie verwerkt welke gegevens? Daarop wordt in dit hoofdstuk ingaan. Er wordt onder meer ingegaan op de functie die SBG vervult, het type gegevens dat wordt verkregen door SBG en van wie SBG die gegevens krijgt, almede op welke wijze die gegevens worden ontvangen en bewerkt en vervolgens door SBG worden doorgegeven. Omdat SBG zal ophouden te bestaan en Akwa haar rol zal overnemen en daarbij de gegevens van SBG - in bewerkte vorm - overgedragen heeft gekregen, wordt ook kort stilgestaan bij de rol van Akwa. In de beoordeling van het handhavingsverzoek dat na dit hoofdstuk zal volgen, zal worden teruggegrepen op de hier beschreven informatiestromen.

3.1 Achtergrond SBG

3.1.1 Doel, activiteiten en taken SBG

Er bestaat voor onder meer zorgaanbieders in de GGZ een wettelijke verplichting[7] tot het leveren van kwalitatief goede zorg. Zorginstituut Nederland is bij wet[8] aangewezen zorg te dragen voor het verzamelen, samenvoegen en beschikbaar maken van informatie over de kwaliteit van verleende zorg. Zorgaanbieders zijn wettelijk verplicht deze informatie te rapporteren aan het Zorginstituut.[9] Om aan onder meer deze verplichting te voldoen is, onder begeleiding van VWS, SBG opgericht door stakeholders (onder meer GGZ Nederland en Zorgverzekeraars Nederland).

Blijkens artikel 3 van haar statuten[10] stelt SBG zich ten doel als een "Trusted Third Party" de geestelijke gezondheidszorg (GGZ) onafhankelijk en betrouwbaar te benchmarken op het gebied van behandeleffect en klanttevredenheid en hiermee door middel van meer transparantie een belangrijke bijdrage te leveren aan het leren en onderzoeken door professionals en instellingen en een kwaliteitsverhogend effect voor de gehele GGZ te bereiken.[11]

SBG heeft verklaard dat zij deze doelstelling verwezenlijkt door middel van vier activiteiten, namelijk: (1) SBG heeft van de aangesloten zorgaanbieders de opdracht gekregen om de wettelijk verplichte prestatie-indicatoren ("meetinstrumenten") door te leveren aan hun toezichthouder, het Zorginstituut Nederland; (2) SBG ontvangt (anonieme) ROM-informatie om mee te benchmarken. Dit benchmarken vindt plaats op twee niveaus, namelijk intra-instelling waardoor een instelling aan interne kwaliteitszorg kan doen en extra-instelling waardoor instellingen zich kunnen vergelijken met elkaar of per regio; (3) Aan SBG is door zorgaanbieders de opslag uitbesteed van een beperkte set geencrypte data, zodat deze beschikbaar kan worden gesteld voor wetenschappelijk onderzoek; (4) SBG heeft in 2015 het verzoek gekregen van GGZ Nederland om ook de Argus-dataverzameling en —rapportage te realiseren voor het GGZ-veld.[12]

[7] Artikel 2 Wet kwaliteit klachten en geschillen zorg. Hieronder bestaat voor zorgaanbieders ook de verplichting tot het op systematische wijze verzamelen en registreren van gegevens betreffende de kwaliteit van de zorg zodat de gegevens voor eenieder vergelijkbaar zijn met gegevens van andere zorgaanbieders van dezelfde categorie, zie artikel 7 lid 2 Wet kwaliteit klachten en geschillen zorg.
[8] Artikel 66d, eerste en derde lid Zorgverzekeringswet
[9] Artikel 66d, tweede lid Zorgverzekeringswet
[10] Zie antwoordbrief SBG van 25 augustus 2017, p. 10, randnummer 38 en bijlage 11 p. 3.
[11] Zie over de doelen nader antwoordbrief SBG van 25 augustus 2017, p. 10 e.v.
[12] Zie o.a. antwoordbrief SBG van 25 augustus 2017, p. 10 e.v.

SBG maakt aldus gegevens uit de zorgsector meetbaar zodat er in de GGZ gebenchmarkt kan worden met als doel de kwaliteit in de zorg te behouden en te verbeteren. SBG doet dit aan de hand van gegevens van verschillende GGZ-aanbieders. GGZ-aanbieders laten patiënten vragenlijsten invullen waarna de ROM-data aangeleverd worden aan de stichting ZorgTTP. ZorgTTP, die handelt in opdracht van de GGZ-aanbieders, is een onafhankelijke derde partij die ondersteuning biedt bij het uitwisselen van databestanden met mogelijk privacygevoelige informatie. Ze levert onder meer technische maatregelen, zoals pseudonimisatie en encryptie. SBG ontvangt daartoe bewerkte gegevens van ZorgTTP.[13]

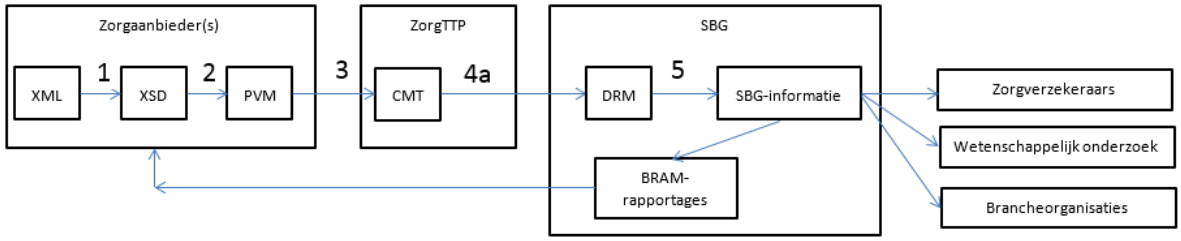
Uit de SBG Aansluitvoorwaarden Zorgaanbieders en het SBG Dataprotocol blijkt dat een zorgaanbieder alle relevante 'Ruwe Data' maandelijks, via een beveiligde omgeving, aan ZorgTTP dient te leveren door middel van een XML-aanlevering. Waarbij de 'Ruwe Data' "*dient te voldoen aan de in de Minimale Dataset geformuleerde technische en inhoudelijke omschrijving*".[14]

Om gegevens aan SBG te leveren dient een zorgaanbieder dus gebruik te maken van ZorgTTP en conform de Minimale Dataset. Dit is een eis die SBG stelt door middel van de Aansluitvoorwaarden en Dataprotocol.

Nadat SBG de door ZorgTTP verwerkte informatie heeft verkregen, wordt de informatie door SBG verder bewerkt en maakt ze die - in de vorm van zogenaamde BRaM-rapportages - beschikbaar aan zorgverzekeraars en GGZ-aanbieders. Hierna wordt nader ingegaan op de gegevensverweking door GGZ-aanbieders, ZorgTTP en SBG.

3.1.2 Informatiestromen en werkwijze SBG

Hierna wordt nader ingegaan op de informatiestromen en de bewerking van de gegevens aan SBG en de wijze waarop SBG de gegevens bewerkt en vervolgens doorgeeft. De gegevensverstrekking vindt beknopt en schematisch weergegeven als volgt plaats[15]:



Gegevensoverdracht GGZ-aanbieders

Patiënten in de GGZ verstrekken aan hun GGZ-aanbieders persoonsgegevens al dan niet via ingevulde vragenlijsten. Een eerste pseudonimiseringsstap vindt plaats in de Privacy- en Verzend Module (PVM) van SBG op locatie bij de GGZ-aanbieder. De gegenereerde gegevens moeten daarbij voldoen aan de specificaties van de minimale dataset (MDS).[16] Alleen als ze voldoen aan deze aanleverstandaard kunnen ze door SBG worden ontvangen. In het document "SBG Minimale Dataset Data aanleverstandaard"[17] is

[13] Vgl.: https://www.zorgttp.nl/. Zie ook antwoordbrief SBG van 25 augustus 2017, p. 32, randnummer 130 e.v.
[14] Zie antwoordbrief SBG van 25 augustus 2017, bijlage 7, p.6 randnummer 5.
[15] Zie ook antwoordbrief SBG van 25 augustus 2017, bijlage 8, p. 4 tot en met 7.
[16] De set aan variabelen zoals overeengekomen door GGZ Nederland en Zorgverzekeraars Nederland, die beschrijft welke (verplichte) inhoudelijke informatie aangeleverd moet worden. Deze variabelen zijn opgenomen in de eerste kolom van de tabel zoals opgenomen in bijlage 2 bij dit rapport. Zie ook bijlage 27 bij antwoordbrief SBG van 25 augustus 2017.
[17] Zie antwoordbrief SBG van 25 augustus 2017, bijlage 9.

omschreven welke gegevens in de MDS verplicht moeten worden opgenomen. Er zijn 29 verplichte gegevenscategorieën die per patiënt ingevuld worden.[18] Er wordt een zogenaamde XSD[19] gebruikt om te controleren of de informatie daadwerkelijk voldoet aan de eisen van de MDS. Hierdoor verlaten alleen gegevens die voldoen aan de eisen van de MDS, de omgeving van de zorgaanbieder.

Bewerkingen binnen PVM
De PVM voert een aantal bewerkingen uit op de ingevoerde data. Vier van de 29 gegevenscategorieën worden gehasht.[20] Dit is het BSN, een koppelnummer, een zorgtrajectnummer en een DBC-trajectnummer. Voor deze vier gegevens ontstaat er, door middel van hashing, een pseudoniem. De overige 25 gegevenscategorieën worden niet bewerkt.

Hierdoor vindt een splitsing plaats van het bestand in een pseudoniemendeel, ook wel sleuteldeel genoemd, en een deel met inhoudelijke data, ook wel datadeel genoemd. Het *sleuteldeel* en *datadeel* worden zodanig versleuteld dat alleen het *sleuteldeel* inzichtelijk is voor ZorgTTP. Het datadeel met inhoudelijk data wordt versleuteld zodat dit niet toegankelijk is voor ZorgTTP. SBG kan het datadeel wel ontsleutelen en dus inzien, deze data acht SBG immers noodzakelijk voor het maken van de BRaM-rapportages. In bijlage 2 bij dit rapport is een tabel opgenomen van vorenstaande gegevensstroom en de toegepaste bewerking.

Gegevensoverdacht ZorgTTP
Na verwerking in de PVM vindt de gegevensoverdacht naar ZorgTTP plaats. Dat gebeurt via een met TLS (Transport Layer Security)-beveiligde verbinding. Deze verbinding zorgt ervoor dat de gegevensstroom die wordt verstuurd tussen de gebruiker en een website of tussen systemen, wordt versleuteld en zo onleesbaar wordt gemaakt voor derden. De versleutelde bestanden worden automatisch verzonden naar de Centrale Module TTP (CMT) van ZorgTTP. Het versleutelde sleuteldeel en datadeel worden ontvangen door de Centrale Module TTP (CMT) bij ZorgTTP. Hierbij beschikt *alleen* de CMT van ZorgTTP over de sleutel om het sleuteldeel te ontsleutelen. Onderstaande tabel maakt dit inzichtelijk:

Sleuteldeel	*Datadeel*
pseudoBSN	Versleuteld en niet inzichtelijk voor ZorgTTP en wordt ook niet aangepast door ZorgTTP.
pseudoKoppelnummer	
pseudoZorgtrajectnummer	
pseudoDBCTrajectnummer	

[18] Dit is exclusief Argus-data en volgt uit de MDS. Argus-data is een landelijke gegevensset voor registratie van vrijheidsbeperkende interventies, zie ook antwoordbrief SBG van 25 augustus 2017, p. 16 en 17.
[19] XSD staat voor XML Schema Definition en beschrijft de structuur van een XML document. In het XML-document ingevulde gegevens kunnen op deze manier gecontroleerd worden op specifieke eigenschappen. Bijvoorbeeld een datum in formaat dd-mm-jjjj, waarbij 19-04-2018 wel wordt geaccepteerd, maar 19-4-18 niet.
[20] Hashen is een verhaspeling of mutatie van gegevens waarbij gebruik wordt gemaakt van een wiskundige functie, ook wel hash-functie genoemd. Een hash-functie heeft de volgende eigenschappen:
- De uitkomst heeft altijd dezelfde vast grootte onafhankelijk van de invoer.
- Het is niet mogelijk om aan de hand van de uitkomst de invoer te verkrijgen. Een hash-functie werkt dus maar één kant op.
- Dezelfde invoer leidt altijd tot exact dezelfde uitkomst. De kleinste verandering (1-bit) leidt tot een totaal andere uitkomst.
- Hash-functie zijn niet persé geheim en voor iedereen toegankelijk en te gebruiken.

Het is daarom mogelijk om voor voorspelbare of veelvoorkomende invoer, de uitvoer te berekenen. Hiermee is een koppeling te maken tussen de invoer en de bijbehorende uitvoer. Dit wordt een koppeltabel genoemd. In een koppeltabel kan de uitkomst worden opgezocht en de daarbij horende invoer.

TRES-deel[21] (niet toegankelijk voor SBG)
[postcodegebied(vier cijfers)]TRES
[geboortelandPatient (o)]TRES
[geboortelandVader (o)]TRES
[geboortelandMoeder (o)]TRES

Vervolgens wordt op de pseudoniemen (de gehashte waardes uit de PVM, zie voorgaande stap) in dit deel door ZorgTTP een tweede pseudonimiseringsslag uitgevoerd. Hierbij wordt gebruik gemaakt van Advanced Encryption Standard (AES). AES is een symmetrisch versleuteling[22] algoritme. In tegenstelling tot hashfuncties wordt er wél gebruik gemaakt van een sleutel om gegevens te versleutelen en ontsleutelen. Dit betekent dat de uitkomst weer kan worden omgezet naar de invoer door gebruik te maken van dezelfde sleutel.

Voor de door ZorgTTP ontvangen pseudoniemen betekent dit het volgende:

- Het pseudoniem, de hashwaarde, wordt versleuteld met een sleutel en daarmee omgezet naar een andere waarde. Deze versleutelde waarde kan daarom (voor SBG) worden gezien als een pseudoniem van het pseudoniem.
- ZorgTTP houdt de gebruikte sleutel voor zichzelf en deelt deze nooit met SBG. Als ZorgTTP deze sleutel wel zou delen, dan zou SBG het versleutelde pseudoniem immers kunnen ontsleutelen.
- ZorgTTP gebruikt iedere keer dezelfde sleutel om de pseudoniemen te versleutelen. Mocht hetzelfde pseudoniem worden aangeleverd, dan zal dit ook leiden tot dezelfde versleutelde waarde.
- ZorgTTP heeft de sleutel en kan de versleutelde waardes weer ontsleutelen tot pseudoniemen (de hashes afkomstig van de zorgaanbieder).

Voor SBG betekent dit het volgende:

- Omdat SBG de sleutel van ZorgTTP niet heeft, kan SBG het pseudoniem van het pseudoniem niet terug (ontsleutelen) naar het pseudoniem zoals bekend in de PVM bij de zorgaanbieder.
- Voor SBG is het niet (zomaar) mogelijk om een koppeltabel te maken. Hiervoor zou medewerking nodig zijn van ZorgTTP of de zorgaanbieder.
- Het blijft voor SBG wel mogelijk om gegevens met hetzelfde pseudoniem (en daarmee horend bij dezelfde persoon) te koppelen met eerder aangeleverde gegevens. SBG zegt hierover het volgende:

"Om de ROM-informatie over het verloop van een behandeling (die gemiddeld langer dan 3 maanden duurt) te kunnen verrijken (met als doel deze te vergelijken), is dus aanlevering op individueel niveau noodzakelijk. Met de moderne eenweg-pseudonimisatie techniek is het mogelijk om zonder sleutel dezelfde patiënt toch telkens hetzelfde pseudoniem te geven."[23]

Na de tweede pseudonimiseringsslag zien de gegevens er voor ZorgTTP er als volgt uit:

Sleuteldeel	*Datadeel*
pseudo[pseudoBSN]	

[21] Deze gegevens worden versleuteld door de ZorgTTP aangeboden TRES-encryptie, waarbij SBG geen toegang krijgt tot de gegevens maar geaggregeerde informatie ervan zien. Zie antwoordbrief SBG van 25 augustus 2017, p. 50.
[22] Symmetrische versleuteling betekent dat dezelfde sleutel wordt gebruikt voor versleuteling als ontsleuteling.
[23] Zie antwoordbrief SBG van 25 augustus 2017, p. 55, randnummer 231.

pseudo[pseudoKoppelnummer]	Versleuteld en niet inzichtelijk voor ZorgTTP en wordt ook niet aangepast door ZorgTTP.
pseudo[pseudoZorgtrajectnummer]	
pseudo[pseudoDBCTrajectnummer]	
TRES-deel (niet toegankelijk voor SBG)	
[postcodegebied(vier cijfers)]TRES [geboortelandPatient (o)]TRES [geboortelandVader (o)]TRES [geboortelandMoeder (o)]TRES	

Vervolgens wordt het sleuteldeel en datadeel klaargezet en opgehaald door SBG via de Data Retour Module (DRM).

Gegevensverwerking door SBG
In de DRM wordt het sleuteldeel en datadeel ontsleuteld. Het sleuteldeel bestaat dus uit de gehashte (in PVM) en vervolgens versleutelde (door ZorgTTP) versies van het BSN, koppelnummer, zorgtrajectnummer en DBCTrajectnummer. Het datadeel bestaat uit de originele gegevens (25 gegevenscategorieën) die bekend zijn van een betrokkene uit een GGZ-aanbieder. In bijlage 2 bij dit rapport wordt dat door middel van een tabel inzichtelijk gemaakt.

De data worden door SBG verzameld in een database en daarna verder verwerkt. De uiteindelijke uitkomsten worden door SBG weergegeven in de BRaM.[24] Met BRaM kan praktijkvariatie in behandeluitkomsten in kaart worden gebracht. Resultaten kunnen met BRaM op verschillende niveaus binnen de GGZ zichtbaar worden gemaakt: het gemiddelde resultaat dat is behaald in geheel Nederland (de 'SBG Benchmark'), het resultaat van een zorgaanbieder, de resultaten van de verschillende locaties van die organisatie, de resultaten van de verschillende afdelingen per locatie en de resultaten van de verschillende behandelaren per afdeling.

3.2 Actuele stand van zaken SBG[25]

Zoals opgemerkt zal SBG ophouden te bestaan en zal haar rol worden overgenomen door Akwa. In dat kader heeft in 2018 een geleidelijke afbouw van de activiteiten en ontmanteling van SBG plaatsgevonden. Er is sprake geweest van een steeds beperktere aanlevering van gegevens door zorgaanbieders en het aantal werknemers van SBG is sterk afgenomen. De laatste medewerker van SBG is op 31 mei 2019 uit dienst getreden. SBG heeft uitsluitend nog een vereffenaar die zorgdraagt voor de vereffening.

Op dit moment worden er geen gegevens meer door zorgaanbieders aan SBG geleverd. SBG heeft daartoe de aansluitvoorwaarden eenzijdig beëindigd en de zorgaanbieders en zorgverzekeraars zijn daarover in december 2018 schriftelijk geïnformeerd. De laatste data aanleveringen aan SBG vonden eind november en eind december 2018 plaats. SBG heeft verklaard dat zij geen beschikking meer heeft over gegevens die door ZorgTTP aan SBG zijn verstrekt. SBG heeft bovendien geen beschikking meer over gegevens die ten grondslag hebben gelegen aan de BRaM-rapportages. De database die SBG in het verleden heeft opgebouwd is reeds vernietigd en dat geldt ook voor back-up bestanden van de database.[26]

[24] Zie daarover nader antwoordbrief SBG van 25 augustus 2017, p. 24 e.v.
[25] Zie antwoordenbrief SBG van 16 januari 2019 en de zienswijze van SBG van 27 juni 2019.
[26] E-mail van 30 april 2019 van Kneppelhout & Korthals N.V. aan de AP.

3.3 Akwa

3.3.1 Doel, activiteiten en taken Akwa

In Akwa - opgericht op 1 juni 2018 - worden de activiteiten van SBG (gedeeltelijk) ondergebracht en voortgezet. Hierbij wordt de infrastructuur voor het aanleveren van gegevens aan SBG overgedragen aan Akwa. Daarnaast wordt de dataset van SBG in 'verarmde' vorm[27] aan Akwa overgedragen. Deze verarming bestaat uit het aggregeren van een drietal variabelen en het verwijderen van tien variabelen. Hieronder wordt uiteengezet wat dit precies betekent ten op zichtte van de dataset van SBG.

De drie categorieën die worden geaggregeerd zijn:

- Geboortejaar, maar alleen voor mensen ouder dan 80 jaar. Alleen die groep krijgen hetzelfde geboortejaar. Iedereen jonger dan 80 jaar wordt niet geaggregeerd en overgedragen aan Akwa.
- Leefsituatie gaat van 8 naar 5 verschillende opties.
- Reden eind DBC gaat van 22 categorieën naar een binaire (twee mogelijkheden) optie.

De volgende tien categorieën worden verwijderd:[28]

- Het pseudoBSN. Hierbij heeft SBG aangegeven dat het volgen van de patiëntlastiger wordt, omdat deze niet gevolgd kan worden over zorgaanbieders heen. Het pseudoBSN blijft namelijk gelijk als je bij instelling A en B een behandeling ondergaat.
- Postcodegebied: *"De versleutelde vier cijfers van de postcode zullen niet worden overgedragen. De afgeleide SES en urbanisatiegraad worden wel overdragen."* De versleutelde vier cijfers zijn met TRES-versleuteld en waren al niet toegankelijk voor SBG. SBG beschikte al over de SES en urbanisatiegraad. Er verandert dus niets ten opzichte van de SBG-dataset met betrekking tot deze categorie.
- Geboorteland patiënt en afgeleide categorieën (Autochtoon, Niet-Westerse allochtoon en westerse allochtoon) daarvan. Deze categorieën waren niet verplicht aan te leveren en zijn optioneel in MDS.
- Geboorteland vader en afgeleide categorieën (Autochtoon, Niet-Westerse allochtoon en westerse allochtoon) daarvan. Deze categorieën waren niet verplicht aan te leveren en zijn optioneel in MDS.
- Geboorteland moeder en afgeleide categorieën (Autochtoon, Niet-Westerse allochtoon en westerse allochtoon) daarvan. Deze categorieën waren niet verplicht aan te leveren en zijn optioneel in MDS.
- Reden non response voor meting.
- Reden non response na meting.
- Aard meting
- Type respondent. Hierover zegt SBG; *"dit gegeven wordt voor de domeinen kinder- en jeugd en dyslexie niet overgedragen. Sinds de inwerkingtreding van de Jeugdwet wordt dit niet meer aangeleverd."*
- Argus data:[29] *"de data-aanlevering is nauwelijks op gang gekomen, zodat het overdragen van deze gegevens niet zinvol is. Bovendien heeft Akwa GGZ geen opdracht om de Argus registratie uit te voeren. Historische vergelijkingen door middel van BRaM-rapportages zullen in de toekomst dus niet meer mogelijk zijn."*

[27] Zie antwoordbrief van SBG van 16 januari 2019. p. 9 en 10.
[28] Zie antwoordenbrief SBG van 16 januari 2019, p. 8 en 9.
[29] Argus is een minimale gegevensset voor de verzameling van gegevens over de toepassing van de meest voorkomende vrijheidsbeperkende interventies in de ggz.

Van deze tien categorieën is er één die aldus niet toegankelijk was voor SBG en drie die optioneel aangeleverd konden worden. Dit betekent dat van de 25 verplichte datapunten die aangeleverd werden aan SBG, er 19 datapunten overgedragen zijn aan Akwa. Akwa staat met de dataset het volgende doel voor ogen: het mogelijk maken van historische vergelijkingen op het gebied van behandeluitkomsten en patiëntervaringen en bijbehorende rapportages te kunnen generen.[30] Daarnaast zal Akwa zelfstandig nieuwe data gaan verzamelen voor benchmarking.

3.3.2 Werkwijze Akwa

Akwa heeft aangegeven dat ze met de GGZ-aanbieder overeen zal komen dat er door de GGZ-aanbieder aan de patiënt uitdrukkelijke toestemming zal worden gevraagd voor het verwerken van zijn/haar gegevens. Deze afspraak zal onderdeel zijn van de overeenkomst tussen Akwa en de GGZ-aanbieders. De keuze daarvoor is ingegeven vanwege de discussies en problematiek die zich rondom SBG en het verwerken van ROM-data heeft voorgedaan en voordoet, niet omdat Akwa van mening is dat de gegevens die ze van de GGZ-aanbieders zal krijgen persoonsgegevens zijn.

Het proces van aanlevering van gegevens aan Akwa zal volgens dezelfde structuur gaan verlopen zoals die werd gebruikt voor de dataverzameling door SBG. Verwezen zij naar hetgeen daarover is opgemerkt in paragraaf 3.1.[31]

[30] Zie antwoordenbrief SBG van 16 januari 2019, p. 9 en 10.
[31] Zie voor een nadere uiteenzetting van de rol en werkwijze van Akwa de antwoordbrief van Akwa van 16 januari 2019.

4. Beoordeling

4.1 Onderzoeksvragen

De kernvraag die in onderhavige casus moet worden beantwoord, is of de gegevens waar het handhavingsverzoek op is gericht kwalificeren als persoonsgegevens . Alleen als dat het geval is, kan de AP beoordelen of de verwerking van persoonsgegevens door SBG in lijn is met de AVG. Daarbij gaat de AP ervan uit dat er - gelet op de door haar overgelegde brief van 19 mei 2017 van haar behandelaar - gegevens van verzoekster volgens het in hoofdstuk 3 beschreven (verwerkings)proces bij SBG zijn binnengekomen.

De AP heeft zich tijdens het onderzoek de volgende vragen gesteld:

- Is de ontvangst van data door SBG een verwerking van persoonsgegevens? Zo ja, is er sprake van persoonsgegevens betreffende de gezondheid?
- Is SBG de verwerkingsverantwoordelijke voor deze verwerking?
- Kan SBG zich beroepen op een wettelijke uitzondering op het verbod van verwerking van persoonsgegevens betreffende de gezondheid?

Verder is nog van belang welk recht van toepassing is; de Wbp of de AVG. Ten tijde van het verzoek om handhaving van 24 maart 2017 gold de Wbp. De Wbp, die de implementatie vormde van richtlijn 95/46/EG[32], is echter ingetrokken op 25 mei 2018[33] en vervangen door de AVG[34] en de UAVG.[35] De AP toetst aan het recht dat nu van toepassing is en dat is de AVG. Daarbij wordt echter opgemerkt dat de voor dit onderzoek relevante begrippen in de AVG ten opzichte van de Wbp nagenoeg ongewijzigd zijn gebleven. De AP is dan ook van oordeel dat de toetsing materieel onder de AVG niet anders is dan onder de Wbp.

4.2 Verwerkt SBG (bijzondere) persoonsgegevens

4.2.1 Inleiding

Ter beantwoording van de vraag of SBG bijzondere persoonsgegevens verwerkt zal de AP eerst nagaan of de gegevens die door SBG worden verwerkt kwalificeren als persoonsgegevens, d.w.z. informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de laatstgenoemde kan direct of indirect worden geïdentificeerd). Dit betekent dat natuurlijke personen direct of indirect herleidbaar zouden moeten zijn in de dataset van SBG. Indien er sprake is van persoonsgegevens, dan zal vervolgens worden bekeken of de persoonsgegevens te kwalificeren zijn als persoonsgegevens betreffende de gezondheid. Tenslotte zal de AP nagaan of er sprake is van een 'verwerking' van persoonsgegevens.

4.2.2 Directe herleidbaarheid

Artikel 4, onderdeel 1, van de AVG definieert als persoonsgegeven: 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"). Als identificeerbaar wordt

[32] Richtlijn van het Europees Parlement en de Raad van 24 oktober 1995, Publicatieblad van de Europese Gemeenschappen, 23 november 1995, Nr. L 281/31 (de zogenoemde Privacyrichtlijn).
[33] In artikel 51 van de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) – die in werking is getreden met ingang van 25 mei 2018 – staat dat de Wbp wordt ingetrokken.
[34] Artikel 99, tweede lid, van de AVG bepaalt dat de AVG van toepassing is met ingang van 25 mei 2018.
[35] Bij koninklijk besluit van 16 mei 2018 (Staatsblad 2018, 145) is het tijdstip tot vaststelling van inwerkingtreding van de UAVG vastgesteld op 25 mei 2018. Dit besluit is gebaseerd op artikel 53 van de UAVG waarbij de inwerkingtreding van de UAVG op een bij koninklijk besluit te bepalen tijdstip mogelijk is gemaakt.

beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.'

De definitie maakt onder meer een onderscheid tussen directe en indirecte herleidbaarheid. Hierna wordt daarom eerst nagegaan of de gegevens van SBG direct herleidbaar zijn tot een natuurlijk persoon en vervolgens of mogelijk sprake is van indirecte herleidbaarheid.

Zoals reeds in paragraaf 3.1 benoemd, verstrekken zorgaanbieders via ZorgTTP gegevens aan SBG. SBG haalt deze gegevens op bij ZorgTTP via de Data Retour Module (DRM). Deze gegevens bestaan uit een sleuteldeel en een datadeel. Het sleuteldeel bestaat uit de gehashte (in PVM) en vervolgens versleutelde (door ZorgTTP) versies van het BSN, koppelnummer, zorgtrajectnummer en DBCTrajectnummer. Het datadeel bestaat uit de originele gegevens (25 gegevenscategorieën) die bekend zijn van een betrokkene uit een GGZ-aanbieder. Voorbeelden van deze gegevens (die ook in bijlage 2 volledig staan vermeld) zijn geslacht, geboortejaar, zorgaanbiedernaam, start en einddatum zorgtraject.

De AP heeft vastgesteld dat in de ontvangen data door SBG geen gegevens staan die directe herleidbaarheid mogelijk maken van geïdentificeerde natuurlijke personen. In de dataset van SBG staan namelijk geen gegevens zoals de volledige naam, adres en/of geboortedatum van natuurlijke personen. Uit het vorenstaande kan naar het oordeel van de AP aldus worden opgemaakt dat geen sprake is van directe herleidbaarheid.

4.2.3 Wijze van anonimiseren door SBG en indirecte herleidbaarheid

Nu naar het oordeel van de AP geen sprake is van directe herleidbaarheid, dient zich vervolgens de vraag aan of mogelijk sprake is van indirecte herleidbaarheid waardoor een natuurlijke persoon wordt geïdentificeerd en dientengevolge sprake is van persoonsgegevens.

Die vraag zal de AP beantwoorden aan de hand van het bepaalde in overweging 26 van de considerans van de AVG en overweging 26 van de considerans van de Richtlijn 95/46/EC. In beide overwegingen is aangegeven dat de beginselen van gegevensbescherming voor elk gegeven betreffende een geïdentificeerde of identificeerbare (natuurlijke) persoon moeten gelden. Daarnaast is aangegeven dat deze beschermingsbeginselen niet van toepassing zijn op (kort gezegd) anonieme gegevens.

Hierna zal de AP de vraag beantwoorden of de data die SBG heeft ontvangen anonieme gegevens betreft, meer specifiek of deze gegevens voldoende geanonimiseerd zijn waardoor indirecte herleidbaarheid naar betrokkenen niet meer mogelijk is. In de opinie van de Groep Gegevensbescherming Artikel 29 over anonimiseringstechnieken (WP 216 advies 05/2014)[36] is nader ingegaan op de vraag wanneer sprake is van dusdanige anonimisering zodat geen sprake meer is van indirecte herleidbaarheid.

Risico's bij het anonimiseringsproces

In de eerder aangehaalde opinie van de Groep Gegevensbescherming Artikel 29 over anonimiseringstechnieken (WP 216 advies 05/2014)[37] gaat de Groep in op vaak gemaakte fouten bij pseudonimisering. Een van de genoemde fouten is dat het verwijderen of vervangen van één of meerdere

[36] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf
[37] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf

attributen[38] zou leiden tot een anonieme dataset. In de praktijk blijken echter nog voldoende quasi-identificatoren[39], andere waarden of attributen aanwezig te zijn waarmee een persoon kan worden geïdentificeerd. De Groep noemt een aantal stappen waarmee een dataset wel als anoniem kan worden beschouwd, zoals "*attributen wegnemen en generaliseren, de oorspronkelijke gegevens verwijderen of op zijn minst samenvoegen tot op een hoog aggregatieniveau.*"

In de bovengenoemde opinie over anonimiseringstechnieken wordt het volgende gesteld over een doeltreffende anonimiseringsoplossing:

"Een doeltreffende anonimiseringsoplossing verhindert dat een persoon in een dataset wordt geïndividualiseerd, dat twee records in een dataset (of in twee afzonderlijke datasets) met elkaar in verband worden gebracht en dat uit die dataset informatie wordt afgeleid. In het algemeen is het verwijderen van direct identificerende gegevens op zich dus niet voldoende om zeker te stellen dat de betrokkene niet langer identificeerbaar is. Doorgaans moeten verdergaande maatregelen worden genomen om identificatie te voorkomen. Een en ander hangt opnieuw af van de omstandigheden en de doeleinden van de verwerking waarvoor de anonieme gegevens zijn bestemd." (onderstreping door AP)

Verderop gaat de opinie in op drie risico's die van belang zijn bij een anonimiseringsproces:

- *"herleidbaarheid, zijnde de mogelijkheid om een persoon in de dataset te individualiseren door sommige of alle records uit te lichten;*
- *koppelbaarheid, zijnde de mogelijkheid om ten minste twee records over dezelfde betrokkene of groep betrokkenen met elkaar in verband te brengen (in dezelfde database of in twee verschillende databases). Wanneer een aanvaller (bijvoorbeeld door de correlatie te analyseren) kan vaststellen dat twee records aan een en dezelfde groep personen zijn gerelateerd, zonder personen binnen deze groep te kunnen individualiseren, dan doorstaat de techniek de „herleidbaarheidstoets", maar niet de koppelbaarheidstoets;*
- *deduceerbaarheid, zijnde de mogelijkheid om de waarde van een persoonskenmerk („attribuut") met grote waarschijnlijkheid af te leiden uit de waarden van een reeks andere attributen."*

Als deze risico's in voldoende mate worden gemitigeerd of uitgesloten dan is de gebruikte anonimiseringsoplossing "*in voldoende mate bestand tegen re-identificatie op basis van de meest waarschijnlijke en redelijke middelen die worden gebruikt door de voor de verwerking verantwoordelijke en enige derde."*

Mitigatie van risico's voor de dataset van SBG

De dataset van SBG bestaat bij ontvangst per record[40] uit vier gepseudonimiseerde attributen en 25 normale attributen. Zoals reeds in paragraaf 3.1.2. vermeld zijn zorgaanbieders verplicht om alle 29 attributen aan te leveren. Kijkend naar deze dataset, voor dat deze wordt verwerkt tot een benchmark, dan kan het volgende worden opgemerkt over de bovengenoemde risico's.

Herleidbaarheid:
Het individualiseren van een record of persoon is mogelijk op een aantal manieren:

- Op basis van het gepseudonimiseerde BSN zou een uniek record uit de dataset gelicht kunnen worden. Het gepseudonimiseerde BSN is immers een unieke identificator.

[38] Een persoonskenmerk. Bijvoorbeeld het geboortejaar, met de bijbehorende waarde '2013'. Zie hiervoor pagina 13 van WP29 opinie advies 5/2014 over anonimiseringstechnieken.
[39] Een quasi-identificator is een combinatie van attributen die verband houden met een betrokkene of groep betrokkenen. Zie hiervoor pagina 13 van WP29 opinie advies 5/2014 over anonimiseringstechnieken.
[40] Een record is gerelateerd aan één betrokkene en bestaat uit een reeks waarden voor elk attribuut. Zie hiervoor pagina 13 van WP29 opinie advies 5/2014 over anonimiseringstechnieken.

- De combinatie van de andere gepseudonimiseerde attributen (koppelnummer, zorgtrajectnummer, DBCtrajectnummer) is mogelijk uniek genoeg om een uniek record uit de dataset te lichten.
- De combinatie van de overige (niet gepseudonimiseerde) attributen is mogelijk ook uniek genoeg om een uniek record uit de dataset te lichten.
- De combinatie van alle attributen (zowel gepseudonimiseerd als niet-gepseudonimiseerd) zijn uniek genoeg om een record uit de dataset te lichten.

Koppelbaarheid:
Voor het opstellen van de SBG Benchmarkrapportages is het volgens SBG nodig om patiënten door de tijd heen te volgen en informatie af te leiden over het succes van een behandeling bij een bepaalde behandelaar.[41] Hierdoor is het nodig om nieuwe informatie te koppelen aan al bij SBG bekende informatie over die individu.

Deduceerbaarheid:
Informatie zoals geslacht, geboortejaar en psychisch welzijn (aan de hand van de Primaire Diagnosecode en Nevendiagnosecode) is per record af te leiden. Daarnaast is grofweg het woongebied af te leiden, omdat gegevens over de zorginstelling ook bekend zijn.

Het is dus inherent aan deze manier van het maken van benchmarks door SBG, dat de risico's met betrekking tot herleidbaarheid, koppelbaarheid en deduceerbaarheid niet weggenomen kunnen worden.

Technische waarborgen dataset SBG

In de opinie over anonimiseringstechnieken schrijft de Groep Gegevensbescherming Artikel 29 dat randomiseren en generaliseren twee manieren zijn waarop anonimisering kan worden benaderd.

Onder randomiseren vallen een groep technieken *"waarmee de waarheidsgetrouwheid van gegevens wordt gewijzigd met het doel die gegevens los te koppelen van de persoon. Als de gegevens voldoende at random zijn (dat wil zeggen willekeurig of onbepaald), is het niet langer mogelijk om ze te herleiden tot een specifieke persoon."*[42]

Randomisatietechnieken op zich helpen niet om het risico op herleiding te verminderen, maar kunnen een uitkomst bieden bij de risico's van deduceerbaarheid. Voorbeelden van dit soort technieken zijn:

- Ruistoevoeging: attributen in de dataset worden gewijzigd zodanig dat deze minder nauwkeurig zijn.
- Permutatie: attributen in de dataset worden van plaats verwisselt zodanig dat deze worden gekoppeld aan andere betrokkenen.
- Differentiële privacy: een techniek die de verwerkingsverantwoordelijke toepast op de gegevensbevragingen (query's) gedaan door een specifieke derde en resulteert in een anonieme dataset, als antwoord op de bevraging. In tegenstelling tot het vrijgeven van de gehele dataset.

Met generaliseren wordt bedoeld de groep anonimiseringstechnieken waarbij de attributen van betrokkenen worden veralgemeniseerd of afgezwakt door de schaalgrootte of omvang te wijzigen. Hiermee kan herleiding tot de persoon worden uitgesloten, maar dienen verdere technieken toegepast te worden om koppelbaarheid en deduceerbaarheid tegen te gaan. Voorbeelden van generalisatietechnieken:

[41] Zie antwoordbrief SBG van 25 augustus 2017, bijlage 27 over de uitleg van het Pseudo-BSN.
[42] Zie hiervoor pagina 14 van WP29 opinie advies 5/2014 over anonimiseringstechnieken.

- K-anonimiteit: het "*voorkomen dat een betrokkene wordt geïndividualiseerd door die samen te voegen met ten minste k andere personen."* Bijvoorbeeld het generaliseren van individuele geboortedata naar geboortejaar.
- L-diversiteit en T-gelijkenis: L-diversiteit zegt iets over de verdeling van de attributen binnen een specifieke groep van personen (equivalentieklassen). Deze verdeling dient zodanig gelijk verdeeld te zijn dat een aanvaller met kennis over de achtergrond van een betrokkene altijd te maken heeft met een hoge mate van onzekerheid. T-gelijkenis is hier een verfijndere vorm van. Uiteindelijk moeten deze methoden het risico op herleidbaarheid en deduceerbaarheid voorkomen, waarbij het niet langer mogelijk is om met een probabilistische aanval een persoon te herleiden dan wel specifieke informatie af te leiden is over een persoon.

Uit de door de AP ontvangen documentatie blijkt dat er geen gebruik wordt gemaakt van enige vorm van randomisatietechnieken op het moment dat SBG de dataset ontvangt. Met betrekking tot generaliseren is de techniek van aggregeren (niet k-anonimiteit) wel gezien, maar foutief toegepast. Zo wordt bijvoorbeeld niet de geboortedatum opgeslagen in de dataset, maar het geboortejaar. Echter is het geboortejaar niet de enige quasi-identificator. Er zijn namelijk 25 quasi-identificatoren, waardoor er binnen de groep van hetzelfde geboortejaar nog steeds individualisatie mogelijk is, zoals locatie zorgaanbieder, geslacht, startdatum, einddatum, etc. Hierdoor is er onvoldoende rekening gehouden met eigenschappen van k-anonimiteit en L-diversiteit.

Met andere woorden, de dataset van SBG is in zoverre gedetailleerd dat er op één of meerdere attributen, gepseudonimiseerd of niet, een selectie kan plaatsvinden zodanig dat er één individu uit de dataset gelicht kan worden. Hierdoor is dus onvoldoende rekening gehouden met de risico's op herleidbaarheid, koppelbaarheid en deduceerbaarheid en kan het niet gaan over een anonieme dataset.

Gepseudonimiseerde gegevens bij SBG

De WP 29 opinie over anonimiseringstechnieken zegt het volgende over pseudonimisering:

Bij pseudonimisering wordt één attribuut (dat doorgaans uniek is) in een record vervangen door een ander attribuut. De natuurlijke persoon is dus nog steeds indirect identificeerbaar. Bijgevolg is pseudonimisering op zich niet voldoende om een dataset volledig anoniem te maken.

Pseudonimisering vermindert de koppelbaarheid tussen een dataset en de oorspronkelijke identiteit van een betrokkene, en is als zodanig een nuttige beveiligingsmaatregel, maar geen anonimiseringsmethode.

De pseudonimiseringsmethode die SBG gebruikt ziet op een combinatie van een hashfunctie en encryptie met een geheime sleutel. Een hashfunctie heeft "*voor een invoer van willekeurige omvang (één enkel attribuut of een verzameling van attributen) een uitvoer met vaste grootte, en kan niet worden teruggedraaid."* Bij encryptie met een geheime sleutel *"kan degene die de sleutel bezit elke betrokkene eenvoudig opnieuw identificeren door de dataset te decoderen".*

Door de combinatie van deze twee methoden worden de risico's op terugdraaien of decoderen verminderd, namelijk:

- De geheime sleutel is bekend bij een trusted third party (ZorgTTP) die deze niet deelt met SBG of enig andere partij. Decodering door SBG is daarmee niet mogelijk en SBG kan dus niet beschikken over de gehashte versies van het BSN, koppelnummer, DBCTrajectnummer en Zorgtrajectnummer.

- De hashfunctie zorgt ervoor dat de trusted third party (ZorgTTP) niet beschikt over de originele waarden van het BSN, koppelnummer, DBCTrajectnummer en Zorgtrajectnummer, maar alleen over de gehashte versies daarvan.
- Door de combinatie is het voor SBG niet mogelijk een koppeltabel te bouwen van alle BSN's[43] met de bijbehorende gehashte waardes.

Echter, de uitkomsten van dit pseudonimiseringsproces zijn per uniek BSN, koppelnummer, DBCTrajectnummer en Zorgtrajectnummer altijd hetzelfde. Met andere woorden, iedere invoer levert altijd exact dezelfde uitvoer. Dit zorgt ervoor dat door de tijd heen nieuwe informatie toegevoegd kan worden aan de al bekende informatie bij SBG.

De eerder genoemde risico's (herleidbaarheid, koppelbaarheid en deduceerbaarheid) worden met het onderhavige pseudonimiseringsproces in onvoldoende mate weggenomen. Zo is herleidbaarheid tot de persoon nog steeds mogelijk doordat de persoon nu geïdentificeerd wordt door een unieke waarde na pseudonimisering. Aangezien dezelfde unieke (gepseudonimiseerde) waarden door de tijd samengevoegd dienen te worden is risico op koppelbaarheid even groot. Gelet op de hoeveelheid gegevens die per pseudoniem worden opgeslagen en de unieke combinatie die dit oplevert blijft het mogelijk een persoon te identificeren op basis van deze gegevensset. De dataset bij SBG is daarmee een gepseudonimiseerde dataset. Het standpunt van SBG dat het geen persoonsgegevens ontvangt en/of verwerkt acht de AP als onjuist.[44]

Conclusie

SBG heeft op hun gepseudonimiseerde dataset onvoldoende technische waarborgen en/of maatregelen genomen om de risico's op herleidbaarheid, koppelbaarheid en deduceerbaarheid in voldoende mate weg te nemen om te kunnen spreken van een anonieme dataset. Het risico op indirecte herleidbaarheid wordt daarom, met deze technische maatregel, in onvoldoende mate weggenomen.

Hiermee beschikt SBG over een gepseudonimiseerde dataset met persoonsgegevens die wordt gebruikt voor het maken van benchmarkrapportages.

4.2.4 Persoonsgegevens betreffende de gezondheid

In de vorige paragraaf heeft de AP vastgesteld dat de dataset die SBG ontvangt persoonsgegevens bevat. In verband met het verbod van verwerking van persoonsgegevens over gezondheid staat hierna de vraag centraal of de gegevens die SBG heeft ontvangen persoonsgegevens zijn over de gezondheid.

Artikel 4, onderdeel 15, van de AVG geeft de volgende definitie van 'gegevens over gezondheid': 'persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven'

Persoonsgegevens over gezondheid omvatten alle gegevens die betrekking hebben op de gezondheidstoestand van een betrokkene en die informatie geven over de lichamelijke of geestelijke gezondheidstoestand van de betrokkene in het verleden, het heden en de toekomst. Dit kan informatie zijn over aan een natuurlijke persoon toegekend cijfer, symbool of kenmerk dat als unieke identificatie van die

[43] Het BSN is een voorspelbare reeks getallen.
[44] Zie antwoordbrief SBG van 25 augustus 2017, p. 44 e.v.

natuurlijke persoon geldt voor gezondheidsdoeleinden en informatie over bijvoorbeeld ziekte, handicap, ziekterisico of medische voorgeschiedenis etc.[45]

De AP stelt vast dat de dataset die SBG (via ZorgTTP) van zorgaanbieders heeft ontvangen persoonsgegevens bevat over de gezondheid. De dataset bevat bijvoorbeeld de naam van de zorgaanbieder en de start en einddatum van een zorgtraject. Zorgaanbieders dienen daarnaast ook de Primaire diagnosecode te verstrekken. SBG kan deze code naast de codelijsten die het bezit zijn van SBG leggen waarna de diagnoses, zoals depressie of borderline, kenbaar zijn voor SBG. Ook het enkele feit dat SBG data ontvangt van GGZ-zorgaanbieders over betrokkenen geeft al aan dat de gegevens betrekking hebben op de gezondheid. Deze data, of het nu in de vorm is van tekst of aan een natuurlijk persoon toegekend cijfer, heeft aldus betrekking op de geestelijke gezondheid van betrokkenen.

De AP stelt vast dat de data die SBG (via ZorgTTP) van zorgaanbieders heeft ontvangen persoonsgegevens bevat over de gezondheid in de zin van artikel 4, onderdeel 15, AVG.

4.2.5 Verwerking

De AVG is van toepassing op de verwerking van persoonsgegevens. De AP stelt vast dat de ontvangst en bewaring van de dataset door SBG een verwerking is in de zin van artikel 4, onderdeel 2, AVG. SBG heeft deze dataset via een digitale verbinding bij de Data Retour Module (DRM) opgehaald en opgeslagen. Daarmee is er sprake van een geautomatiseerd proces die aldus te kwalificeren valt als een verwerking onder de AVG.

4.2.6 Tussenconclusie

Op grond van het bovenstaande komt de AP tot de conclusie dat de data die SBG van zorgaanbieders ontvangt persoonsgegevens over de gezondheid zijn in de zin van artikel 4, onderdeel 1 en 15, AVG. Daarnaast is de ontvangst en bewaring van de dataset door SBG een verwerking is in de zin van artikel 4, onderdeel 2, AVG.

4.3 Is SBG verwerkingsverantwoordelijke?

Hiervoor is uiteengezet dat het ontvangen en bewaren van de dataset door SBG een verwerking van persoonsgegevens is. In het kader van de vraag of deze verwerking in lijn is met de AVG is van belang of SBG is aan te merken als verwerkingsverantwoordelijke.

Artikel 4, onderdeel 7, van de AVG geeft de volgende definitie van 'verwerkingsverantwoordelijke': 'een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (…)'

Bij bestuurlijk akkoord van 2010 is besloten om SBG op te richten voor het verzamelen van informatie over behandeluitkomsten in de GGZ.[46] SBG is een stichting die bestaat uit een bestuur, wetenschappelijke-, gebruikers- en expertraad.[47]

[45] Zie AVG overweging 35.
[46] Zie antwoordbrief SBG van 25 augustus 2017, p. 4.
[47] Zie antwoordbrief SBG van 25 augustus 2017, bijlage 3.

SBG heeft voor het bewerkstelligen van haar doelen verschillende voorwaarden en protocollen opgesteld. Zo zijn in de aansluitvoorwaarden van SBG de randvoorwaarden vastgelegd waaraan zorgaanbieders dienen te voldoen om van de diensten van SBG gebruik te mogen maken. Een van de randvoorwaarden is een door SBG opgestelde dataprotocol. In het dataprotocol is de aard en specificaties van de ruwe data, het niveau waarop de ruwe data betrekking heeft, de wijze van aanlevering als het tijdstip van aanleveren en de minimale vereiste data bepaald. Hoewel zorgaanbieders verantwoordelijk zijn voor de integriteit en validiteit van de aangeleverde data, is SBG verantwoordelijk voor de ontwikkeling, beheer, correct analyseren en verstrekking van de SBG-informatie aan zorgaanbieders en zorgverzekeraars. SBG heeft daarnaast het recht audits uit te laten voeren op de validiteit van de data en de integriteit van het proces van de aanlevering. En SBG faciliteert zorgaanbieders ten aanzien van het inrichten van de activiteiten, processen en procedures.[48]

SBG heeft mede een kwaliteitsdocument opgesteld. In het kwaliteitsdocument is vastgelegd aan welke kwaliteitseisen (normen) SBG moet voldoen. Zo heeft SBG een kwaliteitsfunctionaris en kwaliteitscyclus opgericht, en worden er audits gedaan op de kwaliteit van informatiebeveiliging, privacy, de dienstverlening en realisatie van SBG informatie.[49] De directie van SBG is eindverantwoordelijke voor het informatiebeveiligingsbeleid welke van toepassing is op de kantooromgeving, medewerkers en gegevensuitwisseling met organisaties en personen.[50]

SBG gebruikt de ontvangen data van zorgaanbieders niet alleen voor het maken van de benchmark maar ook voor de doorontwikkeling en kwaliteitsverbetering van de benchmarkrapportages en het ondersteunen van (wetenschappelijke) onderzoeken inzake behandeluitkomsten in de geestelijke gezondheidszorg.[51]

Op basis van het bovenstaande komt de AP tot de conclusie dat SBG als verwerkingsverantwoordelijke valt te kwalificeren in de zin van artikel 4, onderdeel 7, AVG. SBG bepaalt immers op hoofdlijnen en detailniveau welke data en op welke manier deze data binnenkomen bij SBG. Zorgaanbieders die niet de aansluitvoorwaarden van SBG accepteren kunnen geen diensten afnemen van SBG. Daarnaast heeft SBG verregaande verantwoordelijkheden en beslisbevoegdheden over de ontvangen dataset, zoals de validiteit en beveiliging ervan. Dit maakt dat SBG zelfstandig belangrijke beslissingen kan nemen over de dataset die zij via ZorgTTP ontvangt van zorgaanbieders en daardoor als verwerkingsverantwoordelijke aangemerkt wordt.

4.4 Kan SBG zich beroepen op een wettelijke uitzondering op het verbod van verwerking van persoonsgegevens betreffende de gezondheid?

De AP heeft vastgesteld dat de data die SBG (via ZorgTTP) van zorgaanbieders heeft ontvangen persoonsgegevens bevat over de gezondheid en dat SBG hier de verwerkingsverantwoordelijke voor is. Op grond van artikel 9, eerste lid, AVG is het in beginsel verboden om gegevens over gezondheid te verwerken. Dit verbod is niet van toepassing indien SBG zich kan beroepen op een wettelijke uitzonderingsgrond uit artikel 9 AVG jo. artikel 22 tot en met 30 UAVG.

[48] Zie antwoordbrief SBG van 25 augustus 2017, bijlage 7 en 8.
[49] Zie antwoordbrief SBG van 25 augustus 2017, bijlage 10.
[50] Zie antwoordbrief SBG van 25 augustus 2017, bijlage 20.
[51] Zie antwoordbrief SBG van 25 augustus 2017, bijlage 8.

De AP stelt ten eerste vast dat SBG geen beroep kan doen op één van de algemene uitzonderingsgronden in de zin van artikel 9 tweede lid, AVG en artikel 22 en 23 UAVG. Voor zover relevant in dit onderzoek heeft SBG geen uitdrukkelijke toestemming gevraagd voor de verwerking aan de betrokkenen, waardoor een beroep op artikel 9, tweede lid, sub a AVG jo. artikel 22, tweede lid, sub a UAVG niet slaagt.

SBG kan mede geen succesvol beroep doen op de wettelijke uitzonderingsgrond voor wetenschappelijk of historisch onderzoek of statistische doeleinden in de zin van artikel 9, tweede lid, onderdeel j AVG jo. artikel 24 UAVG. Nog in het midden gelaten of het verwerken van gezondheidsgegevens noodzakelijk is voor de doelstellingen van SBG, is het mogelijk om uitdrukkelijk toestemming te vragen aan de betrokkenen ex. artikel 24 sub c UAVG. Toestemming had bijvoorbeeld gevraagd kunnen worden aan de betrokkenen bij het invullen van de vragenlijsten.

Tenslotte kan SBG zich niet beroepen op één van de wettelijke uitzonderingsgronden inzake gegevens over gezondheid. SBG valt namelijk niet onder de genoemde normadressaten van artikel 30 UAVG waarin deze wettelijke uitzonderingsgronden zijn geregeld. Wellicht ten overvloede, SBG is geen instelling of voorziening die medische zorg aanbiedt. Hierdoor kan SBG zich niet beroepen op artikel 9, tweede lid, sub h AVG jo. artikel 30, derde lid, sub a UAVG waarin o.a. is bepaald dat het verbod op verwerking van gezondheidsgegevens niet van toepassing is op hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk.

De AP komt aldus tot de conclusie dat SBG zich niet kan beroepen op één van de wettelijke uitzonderingsgronden die het verbod om gegevens over gezondheid te verwerken zou kunnen opheffen. Dit heeft tot gevolg dat het voor SBG op grond van artikel 9, eerste lid AVG verboden is om de dataset met daarin persoonsgegevens over de gezondheid te verwerken.

4.5 Overige gronden handhavingsverzoek

Door verzoekster zijn nog een aantal argumenten aangevoerd die hiervoor nog niet aan de orde zijn geweest. De AP zet hierna deze argumenten (voor zover nog relevant) uiteen en voorziet hierin in een reactie.

SBG als Trusted Third Party
Verzoekster betwijfelt of SBG een Trusted Third Party (TTP) is en wijst daarbij op de financieringsconstructie van SBG en de participatie van zorgverzekeraars in SBG.

Ten aanzien van dit argument merkt de AP het volgende op. Nog afgezien of de wijze waarop SBG is ingericht en wordt gefinancierd de conclusie rechtvaardigt dat SBG niet als een TTP kan worden gekwalificeerd, merkt de AP op dat ze gelet op haar taak als toezichthouder op de AVG en in het verleden op de Wbp in dit geval moet beoordelen of SBG persoonsgegevens verwerkt. Nu de AP van oordeel is dat SBG persoonsgegevens over de gezondheid verwerkt en deze gegevens door het verwerkingsverbod niet had mogen verwerken, komt ze aan de vraag of SBG al dan niet een TTP is, niet toe. Dit geldt evenzeer voor door verzoekster in dit kader geopperde twijfels ten aanzien van de beveiliging van de systemen van SBG en de daarvoor geldende certificering.

Sleuteldeel ZorgTTP
Verzoekster stelt in haar handhavingsverzoek dat ze niet weet of het CBS beschikt over de mogelijkheid het sleuteldeel van ZorgTTP te 'decrypten'. In dat verband geeft ze aan dat bij het Diagnose Informatie Systeem (DIS)[52] het CBS wel een sleutel heeft.

De AP kan verzoekster niet volgen in deze redenering. De AP heeft tijdens het onderzoek geen aanwijzingen gevonden waaruit blijkt dat CBS beschikt over de mogelijkheid om het sleuteldeel van ZorgTTP te 'decrypten'. Het versleutelde sleuteldeel en datadeel worden ontvangen door de Centrale Module TTP (CMT) bij ZorgTTP. Hierbij beschikt *alleen* de CMT van ZorgTTP over de sleutel om het sleuteldeel te ontsleutelen.

[52]Het betreft Informatie over diagnoses van patiënten in de ziekenhuiszorg, geestelijke gezondheidszorg en forensische zorg die terecht komt in DIS. DIS wordt beheerd door de Nederlandse Zorgautoriteit. Zie ook: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-nza-mag-diagnosegegevens-uit-dis-beperkt-verstrekken

5. Vooruitblik Akwa

5.1 Overgedragen data zijn persoonsgegevens

Tijdens het onderzoek werd bekend dat SBG haar activiteiten zou gaan staken en een groot deel van haar activiteiten en de door haar verzamelde en bewerkte gegevens zou overdragen aan Alliantie Kwaliteit in de geestelijke gezondheidszorg (Akwa). Dit was voor de AP aanleiding ook onderzoek te verrichten naar de gegevens die door SBG aan Akwa zijn overgedragen. De AP heeft zich hiervoor de vraag gesteld of de overgedragen data aan Akwa persoonsgegevens zijn in de zin van de AVG.

Zoals in paragraaf 3.3.1 uiteengezet draagt SBG een verarmde dataset over aan Akwa. Per record, of wel betrokkene worden van de 25 verplichte attributen (zoals aangegeven in de Minimale dataset), er 19 overgedragen aan Akwa. Onder deze 19 attributen vallen ook het gepseudonimiseerde koppelnummer, DBCTrajectnummer en Zorgtrajectnummer. Dit zijn dus drie van vier gepseudonimiseerde attributen, maar ook de primaire Diagnosecode.

SBG heeft aangegeven dat er drie attributen geaggregeerd worden alvorens over gedragen te worden naar Akwa. Dit zijn geboortejaar, leefsituatie en reden einde DBC. Het geboortejaar wordt echter alleen geaggregeerd voor leeftijden ouder dan 80 jaar. Leeftijden jonger dan 80, worden dus niet aggregeerd overgedragen. Kijkend naar de leeftijd van de Nederlandse bevolking dan is ongeveer 4.5 % 80 jaar of ouder.[53] Het lijkt de AP daarom waarschijnlijk dat de hoeveelheid records bij SBG over mensen dan 80 jaar ook lager ligt dan de hoeveelheid records jonger dan 80 jaar. Het aggregeren over deze specifieke leeftijdscategorie, terwijl de andere geboortejaren met rust worden gelaten, dragen niets tot weinig bij tot het komen van een anoniemere dataset. Het aggregeren van acht naar vijf categorieën met betrekking tot de leefsituatie, is om dezelfde reden niet drastisch genoeg.

Gelet op het feit dat er per record nog 19 verplichte categorieën, waaronder de gepseudonimiseerde varianten van het koppelnummer, DBCTrajectnummer en Zorgtrajectnummer, en het onvoldoende aggregeren van het geboortejaar en leefsituatie; acht de AP dat er onvoldoende technische maatregelen zijn genomen om de risico's op herleiding, koppelbaarheid en deduceerbaarheid te reduceren. De verarmde dataset is daarmee wederom niet geanonimiseerd, maar bevat nog steeds gepseudonimiseerde persoonsgegevens met betrekking tot de gezondheid.

[53] https://opendata.cbs.nl/statline/#/CBS/nl/dataset/7461bev/table?ts=1556799278947, bekeken op 2-5-2019.

6. Conclusie

SBG heeft persoonsgegevens over de gezondheid verwerkt in de zin van artikel 4, onderdeel 1 en 15, van de AVG, dan wel - vóórdat de AVG van toepassing was - in de zin van artikel 2, aanhef en onder a, van de Wbp. Dit omdat de gegevens die SBG ontvangen heeft onvoldoende geanonimiseerd waren waardoor het risico op indirecte herleidbaarheid in onvoldoende mate werd weggenomen. Verder concludeert de AP dat SBG voor deze verwerking zich niet kon beroepen op één van de wettelijke uitzonderingsgronden die het verbod om gegevens over gezondheid te verwerken zou kunnen opheffen. Dit heeft tot gevolg dat het voor SBG op grond van artikel 9, eerste lid, AVG verboden was om de dataset met daarin persoonsgegevens over de gezondheid te verwerken.

7. Zienswijze SBG

SBG heeft op 27 juni 2019 aan de AP haar zienswijze op het rapport kenbaar gemaakt. SBG gaat deels in op de juridische beoordelingen van het rapport en deels op de feitelijke onjuistheden en omissies. Hieronder reageert de AP allereerst op de door SBG gestelde feitelijke onjuistheden en omissies. De aanvulling op de feiten heeft overigens niet geleid tot een andere juridische waardering. De AP merkt verder op dat in het kader van de bezwaarprocedure volledige heroverweging plaatsvindt waarbij ook de gronden/ zienswijze van SBG betrokken worden.

7.1 Zienswijze met betrekking tot feitelijke onjuistheden en omissies

Zienswijze SBG
In algemene zin ontbreekt in het gehele rapport een correcte weergave van de verwerkingsactiviteiten van SBG, zo ontbreekt het onderscheid tussen de vier verschillende gegevensverwerkende activiteiten van SBG geheel.

Reactie AP
De AP heeft de verklaring van SBG over haar vier activiteiten toegevoegd in paragraaf 3.1.1.

Zienswijze SBG
In paragraaf 3.1.1 is aangegeven dat SBG onder begeleiding van VWS is opgericht door stakeholders, onder meer GGZ Nederland en Zorgverzekeraars Nederland. Dit is op zichzelf juist, maar volgens SBG ontbreekt dat destijds ook het Landelijk Platform GGz (LPGGz), de koepel van 20 patiënten- en familieorganisaties en thans MIND, betrokken was bij de oprichting van SBG.

Reactie AP
De AP acht de toevoeging van SBG niet relevant voor het rapport. Zoals SBG in de beantwoording op vragen van de AP van 30 mei 2017 op pagina 1 (voetnoot 1) heeft aangegeven, waren er nog andere 12 partijen betrokken bij de oprichting van SBG. De AP heeft daarom de woorden “onder andere” gebruikt en de toevoeging van al deze partijen heeft geen relevantie voor de onderhavige juridische beoordeling.

Zienswijze SBG
In paragraaf 3.1.1 van het rapport is aangegeven dat BRaM-rapportages aan Zorginstituut Nederland werden verstrekt. Dit is naar de mening van SBG onjuist, Zorginstituut Nederland kreeg geen BRaM-rapportages aangeleverd. BRaM-rapportages werden uitsluitend voor doel 2a en 2b gegenereerd.

Reactie AP
De AP heeft Zorginstituut Nederland verwijderd uit de desbetreffende zin.

Zienswijze SBG
In paragraaf 3.1.2 van het rapport is in de afbeelding Vektis opgenomen als partij waar SBG gegevens aan geleverd zou hebben. Er heeft echter volgens SBG nooit gegevenslevering door SBG aan Vektis plaatsgevonden. Dit was wel de intentie zoals te lezen is in het Dataprotocol bij secundaire doelstelling 2f maar is nooit verwezenlijkt. Daarom was deze gegevensstroom wel opgenomen in de data flow schart van 26 juni 2017, welke is bijgesloten als bijlage 18 bij de antwoordbrief van 25 augustus 2017.

Reactie AP
De AP heeft Vektis verwijderd uit de afbeelding, nu het niet bepalend is voor de onderhavige juridische beoordeling.

Zienswijze SBG
In paragraaf 3.1.2 in voetnoot 19 van het rapport is opgemerkt dat het mogelijk is om voor voorspelbare en veelvoorkomende invoer, de uitvoer te berekenen. Dit is naar de mening van SBG technisch onjuist, een hash is nooit in omgekeerde richting te berekenen ongeacht hoe vaak (veelvoorkomend) een invoer ook is. Er is geen herleidbaar patroon dat tot voorspelbaarheid kan leiden.

Reactie AP
De AP volgt deze zienswijze niet. Er wordt in voetnoot 19 niet gesproken over een herleidbaar patroon dat tot voorspelbaarheid kan leiden. Wellicht is de verduidelijking van de voetnoot in de verkeerde context gelezen. Wat dat betreft merkt de AP het volgende op.
De AP is het eens dat in 'normale' gevallen (hetzij dat er geen cryptografisch zwakke hashfuncties gebruikt worden) een hashfunctie niet omgekeerd kan worden. Met andere woorden het is niet mogelijk om met een uitvoer (de hash) en de gebruikte hashfunctie, te komen tot de oorspronkelijke invoer. Echter, als de invoer een voorspelbaar patroon (bijvoorbeeld een reeks oplopende getallen) of veelvoorkomend is (bijvoorbeeld een eenvoudig wachtwoord) dan kan een tabel met invoer en de bijbehorende hash (de uitvoer) berekend worden. Mocht men een hash hebben, waarvan bekend is dat het een voorspelbare invoer had (bijvoorbeeld één getal uit een oplopende reeks getallen) dan kan men triviaal alle hashes van de gehele getallenreeks opnieuw één voor één hashen. Vervolgens kan de hash worden opgezocht in de zojuist berekende lijst en daarmee is de oorspronkelijke invoer bekend geworden. Met dit proces wordt de hashfunctie herhaald om tot dezelfde uitvoer te komen en vervolgens de invoer te achterhalen (op te zoeken).

Zienswijze SBG
In paragraaf 3.2 van het rapport staat vermeld dat SBG nog maar één medewerker in dienst heeft die dat blijft tot de vereffening is afgerond. Dit is onjuist. De laatste medewerker van SBG is op 31 mei 2019 uit dienst getreden. SBG heeft uitsluitend nog een vereffenaar die zorgdraagt voor de vereffening.

Reactie AP
De AP heeft op 23 mei 2019 het rapport aan SBG verzonden. Het feit dat SBG als onjuist aanvoert heeft pas na deze datum plaatsgevonden. Desalniettemin zal de AP toevoegen dat SBG uitsluitend nog een vereffenaar heeft.

Zienswijze SBG
In paragraaf 4.1 van het rapport staan de onderzoeksvragen vermeld. De onderzoeksvragen zijn volgens SBG onzorgvuldig geformuleerd, onvolledig en niet in de juiste volgorde gesteld.

Reactie AP
De AP volgt deze zienswijze niet. De AP acht de onderzoeksvragen juist en ook in de juiste volgorde gesteld. Zoals in paragraaf 4.2 beschreven heeft de AP beoordeeld of er sprake is van persoonsgegevens, persoonsgegevens betreffende de gezondheid en het begrip verwerking. De vraag welke wettelijke grondslag toepasselijk is moet pas gesteld worden als er sprake is van een verwerking van

persoonsgegevens door een verwerkingsverantwoordelijke én nadat het verbod op de verwerking van bijzondere persoonsgegevens opgeheven kan worden.

Zienswijze SBG
In algemene zin ontbreekt een helder, overzichtelijk en volledig juridisch toetsingskader dat de AP als uitgangspunt heeft genomen bij het beoordelen van de gegevensverwerkende activiteiten van SBG en de rol van SBG daarbij.

Reactie AP
De AP volgt deze zienswijze niet. De AP heeft in verschillende paragrafen, zoals vanaf paragraaf 4.2.2 tot en met 4.4, benoemt op welke wetsartikelen, overwegingen en richtlijnen zij haar bevindingen heeft gebaseerd. Het staat SBG natuurlijk vrij om aan te voeren wat hieraan ontbreekt.

Zienswijze SBG
In algemene zin kan niet worden gesproken van deugdelijke en voldoende onderbouwde conclusies, zeker niet voor wat betreft de kwalificatie van SBG als verwerkingsverantwoordelijke en voor wat betreft het feit dat SBG zich niet kan beroepen op een wettelijke uitzondering op het verbod van verwerking van persoonsgegevens betreffende de gezondheid. Beide conclusies worden getrokken op basis van slechts enkele alinea's. Daarnaast ontbreekt in algemene zin een zorgvuldige beoordeling van de door SBG aangedragen argumenten en van de onderbouwing van de standpunten van SBG.

Reactie AP
Zoals al hierboven genoemd zal de AP in de volgende fase, waar partijen zich mede op een zienswijzezitting kunnen uiten over de bevindingen van de AP, zich beraden op de aangevoerde juridische standpunten en kwalificaties.

7.2 Samenvatting zienswijze SBG

Algemeen
SBG is van mening dat het onderzoeksrapport onvolledig is, onjuiste juridische afwegingen en conclusies bevat en voorts dat de conclusies die in het onderzoeksrapport zijn opgenomen, niet gedragen kunnen worden door de inhoud van het onderzoeksrapport.

Zienswijze SBG verwerkingsverantwoordelijke
Volgens SBG is in het onderzoeksrapport geen (duidelijk) onderscheid gemaakt tussen de vier verschillende gegevensverwerkende activiteiten door SBG.[54] Terwijl deze allen een separate en zorgvuldige juridische kwalificatie verlangen, dit ontbreekt in het rapport geheel.

SBG stelt allereerst dat zij geen verwerkingsverantwoordelijke is voor de vier gegevensverwerkende activiteiten nu SBG geen specifieke juridische bevoegdheid heeft, geen impliciete bevoegdheid en evenmin

[54] De vier gegevensverwerkende activiteiten zijn:
1. SBG heeft van de aangesloten zorgaanbieders de opdracht gekregen om de wettelijk verplichte prestatie-indicatoren ('meetinstrumenten') door te leveren aan hun toezichthouder, het Zorginstituut Nederland.
2a. Benchmarken met (anonieme) ROM-informatie intra-instelling, waarbij een instelling aan interne kwaliteitszorg kan doen
2b. Benchmarken met (anonieme) ROM-informatie extra-instelling, waardoor instellingen zich met elkaar kunnen vergelijken of per regio vergelijkingen kunnen maken
3. Digitale kluis t.b.v. van wetenschappelijk onderzoek. De opslag hiervan is door zorgaanbieder uitbesteed aan SBG.
4. Realiseren van een Argus-dataverzameling en –rapportages voor het GGZ-veld, op verzoek van GGZ Nederland.

de feitelijke invloed heeft om het doel en de middelen voor de verwerking vast te stellen. SBG heeft steeds gehandeld onder de feitelijke invloed van de stakeholders in de GGZ en de wetenschappelijke raad en in opdracht van de zorgaanbieder. SBG merkt aldus op dat het dus (een afvaardiging van) patiënten uit de GGZ, zorgaanbieders én zorgverzekeraars was/waren die gezamenlijk en feitelijk op hoofdlijnen en op detailniveau bepaalden welke data en op welke manier data binnenkwamen bij SBG, waarbij dit bovendien mede werd ingegeven door eisen die volgden uit de wettelijke verplichtingen tot het aanleveren van gegevens aan Zorginstituut Nederland en Argus gegevens. Het hanteren van aansluitvoorwaarden kan evenmin leiden tot de kwalificatie van SBG als verwerkingsverantwoordelijke.

De verregaande verantwoordelijkheden en beslisbevoegdheden over de ontvangen dataset, ten aanzien van validiteit en beveiliging ervan, werden evenmin door SBG zelfstandig uitgeoefend. Steeds werd het handelen van SBG, haar directie en medewerkers, feitelijk ingekaderd door de daarover door patiënten uit de GGZ, zorgaanbieders én zorgverzekeraars gemaakte afspraken. Van zelfstandige en/of doorslaggevende invloed van (de directie van) SBG op het bepalen van de doelen van de gegevensverwerkende activiteiten en de middelen was aldus geen sprake. Indien en voor zover de invloed van SBG met betrekking tot de in te zetten middelen in het kader van de gegevensverwerkende activiteiten voor doel 2 groter was dan die past bij de rol van zuivere verwerker is er hoogstens sprake geweest van gezamenlijke verwerkingsverantwoordelijkheid van de zorgaanbieder(s) en SBG. Concluderend is SBG dus van mening dat zij niet als zelfstandig verwerkingsverantwoordelijke kan worden gekwalificeerd. SBG is te kwalificeren als verwerker van de zorgaanbieder. De aansluitvoorwaarden tussen de zorgaanbieder en SBG zijn te kwalificeren als verwerkersovereenkomst.

Reactie AP
De verwerkingsverantwoordelijke is degene die alleen of samen met anderen het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.[55] SBG verwerkt, zoals hiervoor in dit rapport uiteen is gezet, persoonsgegevens; ze ontvangt persoonsgegevens en stelt eisen hoe die moeten worden aangeleverd en aan de uit te voeren bewerkingen. Dat gebeurt naar het oordeel van de AP op een zodanig (gedetailleerd) niveau dat dit niet bij de rol van een zuivere verwerker past. Daarmee kwalificeert SBG dan ook niet als verwerker, maar als verwerkingsverantwoordelijke. Dat er in de verwerkingsketen naast SBG ook anderen (gezamenlijke[56]) verwerkingsverantwoordelijke of invloed uitoefenen op SBG, laat onverlet dat SBG verwerkingsverantwoordelijke is. Onder verantwoordelijkheid van haar bestuur is SBG, zo blijkt volgt uit het Dataprotocol van SBG, belast met de analyse van de persoonsgegevens die zij via TTP ontvangt alsmede voor het ontwikkelen, beheren en ter beschikking stellen van SBG informatie en gerelateerde applicaties aan de gebruikers.

In het licht van en in aanvulling op het vorenstaande merkt de AP nog het volgende op. SBG is verantwoordelijk voor de opmaak van vergelijkingsinformatie voor zorgverzekeraars, patiëntenorganisaties en zorgaanbieders. Daartoe geeft SBG gedetailleerd aan welke informatie haar door de individuele zorgaanbieders moet worden verstrekt via ZorgTTP om te kunnen meten en te benchmarken. Op basis van de Aansluitvoorwaarden[57] van SBG dient de zorgaanbieder maandelijks alle

[55] Artikel 4, onderdeel 7, van de AVG.
[56] In dit verband wijst de AP erop dat het Hof van Justitie van de Europese Unie (HvJEU) heeft bevestigd dat eventuele gezamenlijke verantwoordelijkheid voor bepaalde gegevensverwerkingen niet afdoet aan de individuele verantwoordelijkheid van één van de (gezamenlijke) verantwoordelijken. Vgl. HvJ EU, C-131/12 (Google Spain SL en Google Inc./Agencia Española de Protección de Datos (AEP)), 13 mei 2014, ro. 40. Elk van de verantwoordelijken is aansprakelijk voor het geheel van de gegevensverwerking en de naleving van de daarmee samenhangende verplichtingen (Kamerstukken II 1997/98, 25 892, nr. 3, p. 58).
[57] De rechtsverhouding tussen een zorgaanbieder en SBG wordt beheerst door de "SBG aansluitvoorwaarden Zorgaanbieders". De Aansluitvoorwaarden bevatten de condities waaraan zorgaanbieder dient te voldoen om van de diensten van SBG gebruik te kunnen

relevante zogenoemde 'Ruwe Data' aan ZorgTTP te leveren. In de Minimale Dataset (MDS) is vastgelegd welke Ruwe Data zorgaanbieders aan ZorgTTP dienen te leveren. De Ruwe Data hebben betrekking op informatie over het bestand, de zorgaanbieder, de patiënt, het zorgtraject, de nevendiagnose, de behandelaar, het DBC-traject[58], de metingen en de items. Om een goed en getrouw beeld te geven van de behandeluitkomsten is de zorgaanbieder verplicht om tevens informatie te verschaffen over het aantal DBC's binnen haar organisatie. Het Dataprotocol van SBG bevat verder instructies aan de zorgaanbieder welke informatie moet worden ingediend en hoe. Het bestuur van SBG kan besluiten het Dataprotocol te wijzigen conform de bepalingen in de statuten.
In het Dataprotocol staat verder welke gegevens aan derden worden verstrekt, onder welke voorwaarden en voor welke doeleinden. In dat kader voorziet het Dataprotocol in een toetsing door het bestuur van SBG, in samenwerking met de wetenschappelijke raad van SBG. Het is dus SBG die bepaalt waar de door haar geanalyseerde (geaggregeerde) gegevens terechtkomen.
Uit het vorenstaande concludeert de AP dat SBG wel degelijk doel van en middelen voor de verwerking van persoonsgegevens en daarmee als verwerkingsverantwoordelijke kwalificeert.[59]

De AP merkt tot slot nog op dat ze niet gehouden een nadere opsplitsing te maken per specifieke gegevensverwerkende activiteit. In dat verband stelt de AP vast dat SBG ten behoeve van de verschillende gegevensverwerkende activiteiten één set data ontvangt waarop de Aansluitvoorwaarden en het Dataprotocol van SBG van toepassing zijn en de persoonsgegevens dienovereenkomstig door SBG worden verwerkt.

Zienswijze SBG wettelijke grondslag en uitzonderingsgronden artikel 9 AVG
Daarnaast stelt SBG dat de AP heeft nagelaten te onderzoeken welke wettelijke grondslagen toepasselijk zijn bij de verwerkingsactiviteiten van SBG. SBG heeft uiteengezet op welke grondslagen de zorgaanbieder zich kan beroepen, nu de zorgaanbieder volgens SBG de verwerkingsverantwoordelijke is voor de gegevensverwerkende activiteiten en SBG, als zuivere verwerker, de gegevensverwerkende activiteiten op basis van de wettelijke grondslag van de zorgaanbieder mag uitvoeren. De zorgaanbieder kan zich volgens SBG voor de meetinstrumenten taak beroepen op artikel 6, eerste lid, sub c AVG. Voor de intra-instelling benchmarken met ROM kan de zorgaanbieder zich beroepen op artikel 6, eerste lid, sub b en c AVG. Voorts kan de zorgaanbieder voor de extra-instelling benchmarken met ROM zich baseren op artikel 6, eerste lid, sub c AVG en potentieel ook op sub b. Wat betreft het aanbieden van de digitale kluis ten behoeve van wetenschappelijk onderzoek kan de zorgaanbieder zich beroepen op artikel 6, eerste lid, sub b AVG. Tenslotte kan de zorgaanbieder voor het bijhouden van de Argus-registratie zich volgens SBG beroepen op artikel 6, eerste lid, sub c AVG.

Voorts voert SBG aan dat niet zij, maar de zorgaanbieder zich op een wettelijke uitzondering op het verbod van verwerking van persoonsgegevens betreffende de gezondheid moet kunnen beroepen. Uitgaande dat er sprake is van persoonsgegevens, kan volgens SBG de zorgaanbieder zich voor de meetinstrumenten taak beroepen op artikel 9, tweede lid, sub i AVG. Voor de intra-instelling benchmarken met ROM kan de zorgaanbieder zich beroepen op artikel 9, tweede lid, sub h AVG juncto artikel 30, derde lid, aanhef en onder sub a UAVG. Wat betreft de extra-instelling benchmarken met ROM, is het mogelijk dat de zorgaanbieder geen beroep kan doen op wettelijke uitzondering van artikel 9, tweede lid, sub h juncto

maken. Daarnaast beschrijven de Aansluitvoorwaarden de rol van SBG als gegevensmakelaar en bevatten die de randvoorwaarden van de door de ggz-aanbieder te verstrekken opdracht aan ZorgTTP.
[58] DBC staat voor Diagnose Behandeling Combinatie
[59] Daarbij is van belang op te merken dat ook als iemand louter de middelen vaststelt, hij verantwoordelijke kan zijn. De Artikel 29-werkgroep geeft in haar voornoemd advies aan dat bij het vaststellen van de middelen alleen van verantwoordelijkheid sprake is wanneer die vaststelling betrekking heeft op de wezenlijke aspecten van de middelen. Vgl. werkgroep "Artikel 29", Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", p. 17.

artikel 30, derde lid, aanhef en onder sub a UAVG. Voor het bewaren van door de zorgaanbieder aan SBG aangeleverde gegevens ten behoeve van wetenschappelijk onderzoek in de digitale kluis, kan de grondslag volgens SBG gevonden worden in artikel 9, tweede lid, sub f AVG. Tenslotte kan de zorgaanbieder voor het bijhouden van de Argus-registratie zich volgens SBG beroepen op artikel 9, tweede lid, sub i AVG.

Reactie AP
De AP volgt SBG niet in haar zienswijze en merkt daarover het volgende op. Omdat SBG naar het oordeel van de AP kwalificeert als verwerkingsverantwoordelijke en niet als verwerker dient ze zelfstanding een vruchtbaar beroep te kunnen doen op een van de uitzonderingsgronden om de haar toevertrouwde persoonsgegevens over gezondheid (een bijzondere categorieën van persoonsgegevens) te kunnen verwerken. [60] De AP heeft gemotiveerd uiteengezet dat SBG dat niet kan.

Zienswijze SBG toestemming en anonimisering
De AP lijkt volgens SBG de suggestie te wekken dat het vragen van uitdrukkelijke toestemming aan de patiënt de enige mogelijkheid is om gezondheidsgegevens in het kader van kwaliteitsregistratie(s) te mogen verwerken. De AP lijkt (impliciet) de 'consent or anonymize benadering' aan te hangen. Deze theorie gaat ervan uit dat ofwel (uitdrukkelijke) toestemming nodig is, ofwel dat gegevens anoniem moeten zijn. Nu de AP de facto de lat voor anoniem zo hoog legt dat dit praktisch onhaalbaar is, kom je vanzelf uit bij (uitdrukkelijke) toestemming. Daarmee is er volgens SBG sprake van een zwart of wit-benadering, zonder de grijstinten daartussen te erkennen. Het miskent bovendien dat aan het vragen van (uitdrukkelijke) toestemming in het kader van gegevensverwerking voor kwaliteitsregistraties ernstige nadelen kleven, alsmede dat volledige anonimisering leidt tot onjuiste uitkomsten. SBG vraagt de AP om dit standpunt nog eens kritisch tegen het licht te houden.

Reactie AP
De AP is, zoals in het rapport uitvoerig is gemotiveerd, van oordeel dat sprake is van (bijzondere) persoonsgegevens. Dat houdt in dat SBG die gegevens alleen mag verwerken als ze zich kan beroepen op een van de uitzonderingsgronden. Nu SBG dat niet kan, betekent dat de betreffende persoonsgegevens alleen met (uitdrukkelijke) toestemming van de betrokkene kunnen worden verwerkt. Dat dit, zoals SBG betoogt, tot ernstige nadelen en onjuiste uitkomsten leidt, is - wat daarvan verder overigens ook zij - een gevolg van de toepasselijke wet- en regelgeving alsmede van de keuzes die zijn gemaakt in het kader de op- en inrichting van SBG. De AP ziet hierin evenwel geen aanleiding om in dit verband een andersluidend standpunt in te nemen.

Zienswijze SBG persoonsgegevens
SBG stelt zich primair op het standpunt dat zij geen persoonsgegevens verwerkt. Volgens SBG kan de door de AP aangehaalde WP29-opinie niet als maatstaf gelden om te bepalen of de gegevens voldoende geanonimiseerd zijn. Naar de mening van SBG zijn er twee andere en met elkaar samenhangende criteria die tot uitgangspunt genomen moeten worden bij de beantwoording van de vraag of gegevens voldoende zijn geanonimiseerd.

Verwijzend naar het Breyer arrest, stelt SBG allereerst dat niet (langer) gesproken kan worden van middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt om de natuurlijke persoon te identificeren als (1) identificatie bij wet verboden is of (2) in de praktijk ondoenlijk is, bijvoorbeeld omdat zij een excessieve inspanning vergt zodat het gevaar voor identificatie in werkelijkheid onbeduidende lijkt. Er is dan geen sprake van indirect herleidbare gegevens en aldus geen sprake van persoonsgegevens.

[60] Zie artikel 9 AVG en de artikelen 22 – 30 UAVG.

Ten tweede is volgens SBG de 'motivated intruder test' relevant die beschreven wordt door de Information Commissioner's Office (ICO), de Britse privacy-toezichthouder, in het document "Anonymisation: managing data protection risk. Code of practice". De relevante vraag is of het voor een gemotiveerde indringer, gelet op diens kennis en voorhanden middelen zoals tijd, geld en mankracht, redelijkerwijs mogelijk is om natuurlijke personen in de geanonimiseerde data die SBG van Stichting ZorgTTP ontvangt te identificeren. Volgens SBG luidt het antwoord op de hiervoor genoemde vraag ontkennend. Bovendien gaat het om de mogelijkheid tot identificeren en niet om de mogelijkheid tot individualiseren. SBG licht dit als volgt toe.

SBG is niet in staat om de versleutelde en gecodeerde attributen uit het door ZorgTTP namens de zorgaanbieder aan SBG verstrekte Bron XML bestand te ontsleutelen. Nu SBG niet in staat geacht kan worden tot het ontsleutelen van de versleutelde en gecodeerde attributen uit het Bron XML bestand dat ZorgTTP oplevert, is het evenmin aannemelijk dat een gemotiveerde indringer tot deze ontsleuteling redelijkerwijs in staat zal zijn. Een gemotiveerde indringer zal de medewerking van ZorgTTP en de zorgaanbieder nodig hebben om tot ontsleuteling en identificatie te komen, welke medewerking uiteraard zal worden onthouden. Zo de gemotiveerde indringer al toegang zou hebben tot de voldoende geanonimiseerde dataset is hij aangewezen op de inzet van onwettige middelen, zoals het hacken of inbreken op de systemen van ZorgTTP en/of de zorgaanbieder, om tot ontsleuteling te komen. De noodzaak tot het inzetten van dergelijke onwettige middelen maakt echter dat er niet langer sprake is van redelijkerwijs in te zetten middelen tot identificatie. Daarom kan volgens SBG niet anders dan geconcludeerd worden dat het Bron XML bestand dat ZorgTTP na bewerking oplevert een voldoende geanonimiseerd bestand is waardoor SBG géén persoonsgegevens ontvangt.

Volgens de AP is het voor SBG mogelijk om, gelet op het gebruik van steeds hetzelfde pseudoniem (van het pseudoniem), een persoon in een dataset te individualiseren. Dit is naar de mening van SBG juist. Vervolgens dringt volgens SBG de vraag zich op of wanneer de mogelijkheid tot individualiseren (en dus niet tot identificeren!) bestaat dit ertoe leidt dat er sprake is van indirecte herleidbaarheid en dus tot de kwalificatie persoonsgegevens. Het antwoord op die vraag luidt volgens SBG ontkennend, terwijl de AP uitgaat van een bevestigend antwoord.

Vervolgens wijst de AP op drie in de opinie genoemde risico's waarop acht moet worden geslagen bij het anonimiseringsproces, te weten de kans op herleidbaarheid, koppelbaarheid en deduceerbaarheid. De AP concludeert na bespreking van de drie risico's dat SBG deze onvoldoende mitigeert. Onder verwijzing naar de Tekst & Commentaar 'Privacy- en telecommunicatierecht' stelt SBG dat het juiste criterium moet zijn of het voor een gemotiveerde indringer, gelet op diens kennis en voorhanden middelen zoals tijd, geld en mankracht, redelijkerwijs mogelijk is om natuurlijke personen in de geanonimiseerde data te identificeren. Door het verkeerde criterium te hanteren om te bepalen of er sprake is van indirect herleidbare gegevens, heeft de AP niet kunnen komen tot de (tussen)conclusie dat SBG persoonsgegevens verwerkte.

Aanvullend benoemt SBG dat ook de Minister van Volksgezondheid, Welzijn en Sport ("VWS") in antwoord op Kamervragen van het lid Leijten (SP) op 23 maart 2017 antwoordde: "Door het beschreven proces zijn de ROM gegevens zodanig bewerkt dat zorgaanbieders aan SBG geen tot de persoon te herleiden informatie aanleveren". Het verbaast SBG dat de AP bij het komen tot haar conclusie dat SBG persoonsgegevens verwerkt deze opmerking van de Minister van VWS over de kwalificatie van de gegevens die SBG verwerkt zonder enige bespreking kennelijk heeft verworpen.

SBG geeft aan zich er over te verbazen dat de AP de conclusies in de door SBG overlegde auditrapporten kennelijk zonder enige bespreking heeft verworpen. Het had op de weg van de AP gelegen om gemotiveerd

aan te geven op grond waarvan de kennelijke verwerping van de conclusies in de twee auditrapporten gebaseerd is.

In 2009 heeft het College Bescherming Persoonsgegevens ("CBP"), de voorloper van AP, in een ander onderzoeksrapport beschreven dat toepassing van pseudonimisering conform vijf voorwaarden leidt tot voldoende geanonimiseerde gegevens. SBG merkt in dit kader op dat het lijkt alsof de AP deze eerder voorgestane benadering impliciet (!) heeft losgelaten. Het kan uiteraard zo zijn dat er nieuwe inzichten ontstaan welke tot gevolg hebben dat een oude benadering niet langer als uitgangspunt heeft te gelden. Het kan echter niet zo zijn dat bij de beantwoording van de vraag of SBG persoonsgegevens verwerkt een nieuwe benadering wordt toegepast, terwijl SBG er blijkens de overgelegde auditrapporten op mocht vertrouwen aan de voorwaarden die onderdeel uitmaakten van de oude benadering te voldoen. Dit levert volgens SBG strijd op met het rechtszekerheidsbeginsel.

Reactie AP
Het verschil van inzicht tussen SBG en de AP spitst zich in de kern toe op de vraag of sprake is indirecte herleidbaarheid. De AP meent dat daarvan sprake is en kan zich dan ook niet verenigen met de zienswijze van SBG. Hierna wordt dat toegelicht.

De gelijkenis die SBG maakt met de uitspraak van het Hof inzake Breyer gaat naar het oordeel van de AP niet op. Deze zaak ziet uitsluitend op de indirecte herleidbaarheid van dynamische IP-adressen. Daarbij is geen aanvullende informatie beschikbaar bij de onlinemediadienstverlener. Hierdoor dient deze zich noodzakelijkerwijs tot de Internet Service Provider te wenden om het dynamische IP-adres te herleiden naar een persoon. Bij SBG is er ten aanzien van elke gepseudonimiseerde patiënt echter veel meer informatie voorhanden. Het betreft niet slechts één datapunt, zoals het geval bij het dynamische IP-adres, maar tientallen.[61] Gelet op het type gegevens en het aantal gegevens dat over één patiënt wordt verwerkt gedurende een langere tijd, is daarmee (het risico op) indirecte herleiding bij meer partijen en publieke bronnen niet te voorkomen. De AP merkt hierbij nog op dat keuze van SBG om patiënten individualiseerbaar te maken in combinatie met de keuze om direct identificerende persoonsgegevens te pseudonimiseren, leidt tot een potentieel kwetsbaar systeem dat een reëel risico op identificatie met zich mee brengt. In dit verband merkt de AP op dat via een verzoek om inzage in persoonsgegeven een betrokkene bij de zorgaanbieder en vervolgens bij SBG op een legitieme wijze herleiding mogelijk kan maken.

Waar SBG verwijst naar de 'motivated intruder test' merkt de AP het volgende op. Ten aanzien van een gemotiveerde indringer met data afkomstig van verschillende zorgaanbieders en die toegang heeft tot de ruwe SBG-database (die zoals reeds opgemerkt een grote hoeveelheid datapunten per pseudoniem bevat) is indirecte identificatie, door middel van het combineren van deze gegevens en rekening houdend met de huidige beschikbare technologie en de constante en snelle ontwikkeling die de technologie doormaakt zeer aannemelijk te achten. Daarbij benadrukt de AP dat SBG als verwerkingsverantwoordelijke nadrukkelijk ook rekening dient te houden met toekomstige situaties en ontwikkelingen. Verwezen zij naar het in dit rapport aangehaalde WP advies 216 05/2014 en overweging 26 van de AVG.

SBG verwijst ook nog naar antwoorden van de minister van Volksgezondheid, Welzijn en Sport op Kamervragen en waarin de minister concludeert dat SBG geen tot de persoon te herleiden informatie aangeleverd krijgt. Dienaangaande merkt de AP op dat ze als onafhankelijke toezichthouder, gelet op de haar toebedeelde taak, zelfstandig en onafhankelijk een beoordeling maakt of sprake is van persoonsgegevens en dit los staat van het oordeel dat de minister daarover heeft en uiteenzet in bijvoorbeeld antwoorden op Kamervragen.

[61] Zie nader daarvoor nader bijlage 2 bij dit rapport.

SBG refereert voorts aan de door externen opgetelde auditrapporten. Voor zover de AP ten aanzien van de vraag of sprake is van verwerking van persoonsgegevens tot een aan andere conclusie komt dan de opstellers van de auditrapporten merkt de AP op dat ze in dit rapport gemotiveerd uiteen heeft gezet waarom ze van mening is dat sprake is van (een verwerking van) persoonsgegevens. De AP ziet tegen die achtergrond geen aanleiding (de conclusies uit) de auditrapporten nog expliciet te weerleggen.

Tot slot verwijst SBG nog naar een brief van het CBP uit 2009. Hierover merkt de AP het volgende op. Als een van de voorwaarden, die noodzakelijk voor de conclusie dat sprake is van voldoende geanonimiseerde gegevens, wordt in de brief van het CBP genoemd dat de verwerkte gegevens niet indirect identificerend mogen zijn. Zoals hiervoor gemotiveerd uiteen is gezet, is daarvan in het geval van de gegevens van SBG nu juist geen sprake. De AP ziet dan ook niet in dat de in de brief van het CBP genoemde voorwaarden zijn losgelaten.

Bijlage 1

Verloop van het onderzoek

Bij brief van 24 maart 2017 heeft verzoekster de AP verzocht om handhavend op te treden tegen SBG. De AP heeft daarop SBG op de hoogte gesteld van het handhavingsverzoek.

Bij brief van 24 april 2017 heeft SBG gereageerd op het handhavingsverzoek.

Bij brief van 1 mei 2017 is aan verzoekster een nadere onderbouwing van het verzoek gevraagd.

Op 23 mei 2017 heeft de AP de gevraagde onderbouwing ontvangen.

Bij brief van 30 mei 2017 heeft de AP aan SBG medegedeeld een onderzoek in te stellen naar de verwerking van persoonsgegevens door SBG. In die brief heeft de AP vragen gesteld aan SBG.
Tevens heeft de AP verzoekster per brief van 30 mei jl. geïnformeerd over de start van dit onderzoek.

Op 2 augustus 2017 is ter zake van de onderhavige problematiek een vonnis in kort geding gewezen, met SBG als verweerster.[62] De voorzieningenrechter oordeelde dat niet voldoende aannemelijk is geworden dat sprake is van de verwerking van persoonsgegevens in de zin van de Richtlijn[63]en de Wbp.

Bij brief van 25 augustus 2017 heeft SBG de vragen van de AP beantwoord.

Op 11 september 2017 is verzoekster per e-mail geïnformeerd over het feit dat de AP nog bezig is met de beoordeling van de ontvangen informatie van SBG en de betekenis van het vonnis in kort geding.

Bij brief van 5 februari 2018 heeft verzoekster schriftelijk aan de AP haar zorgen geuit betreffende de aanlevering van medische data door GGZ-instellingen aan SBG, omdat verzoekster uit de media had vernomen dat een derde van de GGZ-instellingen hiermee was doorgegaan. Hierin zag verzoekster aanleiding de AP te verzoeken om hangende het onderzoek de aanlevering van data aan SBG per direct stil te laten leggen.

Per e-mails van 22 en 31 januari 2018, 17 februari 2018 en 30 maart 2018 heeft verzoekster aanvullende informatie naar de AP gestuurd.

Bij brief van 18 april 2018 heeft verzoekster de AP in gebreke gesteld wegens het uitblijven van een besluit op haar handhavingsverzoek. Op 2 mei 2018 heeft verzoekster de ingebrekestelling ingetrokken.

Op 11 juli 2018 heeft de AP een gesprek gevoerd met SBG waarin door SBG is toegelicht dat zij op korte termijn alleen nog data wil verwerken met toestemming van de patiënt. Die verwerking zou plaats moeten vinden door een onafhankelijk kwaliteitsinstituut.

Op 4 oktober 2018 heeft SBG de AP per e-mail geïnformeerd dat er belangrijke besluiten genomen waren omtrent de toekomst/discontinueren van SBG.

[62] ECLI:NL:RBMNE:2017:4011
[63] Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens

Op 20 november 2018 ontving de AP een schriftelijke ingebrekestelling van verzoekster.

De AP is op 27 november 2018 per brief nader geïnformeerd door SBG omtrent de toekomst/discontinueren van SBG.

Op 3 december 2018 heeft de AP beslist op het handhavingsverzoek. Het handhavingsverzoek is bij dit besluit afgewezen onder de motivering dat het onderzoek naar SBG op dat moment nog niet was afgerond en er derhalve voor de AP geen mogelijkheid bestond om handhavend op te treden tegen SBG.

Dit besluit is op 3 december 2018 per reguliere en aangetekende post aan verzoekster en SBG gezonden en op 9 januari 2019 nogmaals per reguliere en aangetekende post alsmede per e-mail op 8 januari 2019 aan verzoekster, toen bleek dat het aangetekende poststuk niet was afgehaald.

Op 14 december 2018 zijn SBG en Akwa om nadere inlichtingen verzocht.

Op 16 januari 2019 hebben Akwa en SBG de verzochte informatie aangeleverd bij de AP.

Verzoekster heeft op 10 januari 2019 pro forma bezwaar gemaakt tegen het besluit van de AP van 3 december 2018. De AP heeft dit bezwaar op 11 januari 2019 ontvangen.
De AP heeft verzoekster een termijn gegund tot aanvulling van haar gronden eindigend op 13 februari 2019.

Op 5 februari jl. heeft verzoekster laten weten een advocaat ingeschakeld te hebben en om die reden verzocht om vier weken uitstel. De AP heeft dat verzoek ingewilligd bij brief aan verzoekster van 6 februari 2019.

Bij e-mail van 6 februari, 14 maart en 30 april 2019 heeft SBG naar aanleiding van door de haar op 16 januari 2019 verstrekte informatie desgevraagd nog aanvullende informatie verstrekt.

Bijlage 2

1. Gegevensverwerking PVM

In de onderstaande tabel[64] staan drie kolommen. De eerste kolom beschrijft de data vóór verwerking door de PVM, tweede kolom ná de verwerking door de PVM en de derde kolom wat voor verwerking heeft plaatsgevonden. De '(o)' geeft aan dat dit gegeven optioneel kan worden aangeleverd. Met rood is aangegeven welke gegevens verwerkt worden tot pseudoniemen in de PVM en met blauw is aangegeven welke gegevens worden geaggregeerd en versleuteld met TRES. Het rode deel wordt door ZorgTTP het sleuteldeel genoemd en de overige data het datadeel.[65] Het datadeel is niet toegankelijk door ZorgTTP, maar wel voor SBG. Het sleuteldeel en datadeel worden zodanig versleuteld dat alleen het sleuteldeel inzichtelijk is voor ZorgTTP. Het inhoudelijke datadeel (weergegeven in zwart) wordt pas weer inzichtelijk bij SBG tijdens de latere stappen.

Gegevens voor bewerking door PVM[66]	Gegevens na bewerking door PVM	Type verwerking dat heeft plaatsgevonden
Zonder Argus gegevens		
Zorgaanbieder:		
Zorgaanbiedernaam		
Zorgaanbiedercode		
Patiënt:		
BSN	Pseudo BSN	Een BSN wordt gehasht tot pseudoBSN. Het originele BSN wordt verwijderd en niet aangeleverd.
Opleidingsniveau		
Leeftijdsituatie		
geboortelandMoeder (o)	[geboortelandMoeder (o)]TRES Voor SBG wordt dit omgezet in herkomst categorieën: autochtoon, niet-westers allochtoon en westers allochtoon.	Het land is met TRES versleuteld en niet toegankelijk voor SBG. Het wordt wel door SBG opgeslagen.
geboortelandVader (o)	[geboortelandVader (o)]TRES Voor SBG wordt dit omgezet in herkomst categorieën: autochtoon,	Dit is met TRES versleuteld en niet toegankelijk voor SBG. Het wordt wel door SBG opgeslagen.

[64] Samengesteld uit de documenten:
- 20170825 - DEF beantwoording vragen AP, pagina 45 en 46
- Bijlage 18 – Flowchart-data-privacy-SBG-V1_9-20170628
- SBG Minimale Dataset, Data aanleverstandaard inclusief Argusaanlevering, versie 20180701
- Factsheet_pseudonimisatie_ZorgTTP_2017
- Bijlage 27 - MDS uitleg per variabele

[65] Zie Factsheet_pseudonimisatie_ZorgTTP_2017

[66] Dit is gebaseerd op de MDS, de voorbeelden van XML-bestanden (SBG Voorbeeld XML met en zonder Argus) en het XSD-bestand. De documenten zijn te vinden op: https://www.sbggz.nl/Documenten onder Technische Documentatie.

	niet-westers allochtoon en westers allochtoon.	
geboortelandPatient (o)	[geboortelandPatient (o)]TRES Voor SBG wordt dit omgezet in herkomst categorieën: autochtoon, niet-westers allochtoon en westers allochtoon.	Dit is met TRES versleuteld en niet toegankelijk voor SBG. Het wordt wel door SBG opgeslagen.
Postcodegebied [dit zijn de vier cijfers van de postcode]	[postcodegebied(vier cijfers)]TRES Vier cijfers van de postcode worden met TRES versleuteld en zijn niet inzichtelijk voor SBG, zie stap 4b. Voor SBG wordt de postcode omgezet naar SES-waarde en Urbanisatiegraad.	*"Deze worden door ZorgTTP nog vóór ontvangst bij SBG TRES-geëncrypteerd en geaggregeerd tot twee belangrijke casemixvariabelen namelijk Urbanisatiegraad (5 groepen) en Sociaal Economische Status (5 groepen). SBG ontvangt dus geen postcode."*
Geslacht		
Geboortejaar		
Koppelnummer	Pseudo Koppelnummer	Een koppelnummer wordt gehasht tot pseudokoppelnummer. Het origineel wordt verwijderd en niet aangeleverd.
Zorgtraject		
einddatumZorgtraject		
startdatumZorgtraject		
GAFscore		
primaireDiagnoseCode		
Locatiecode (o)		
zorgdomeinCode		
zorgtrajectnummer	Pseudo zorgtrajectnummer	Een zorgtrajectnummer wordt gehasht tot pseudozorgtrajectnummer. Het origineel wordt verwijderd en niet aangeleverd.
Nevendiagnose code		
nevendiagnoseCode		
Behandelaar		
Beroep (o)		
Alias (o)		
primairofNeven (o)		
DBCTraject[67]		
redenEindeDBC		

[67] Er kunnen meerdere DBC-trajecten per patiënt worden opgegeven

datumLaatsteSessie		
datumEersteSessie		
einddatumDBC		
startdatumDBC		
DBCPrestatieCode		
RedenNonResponseVoormeting		
RedenNonResponseNameting		
DBCTrajectnummer	Pseudo DBCTrajectnummer	Een DBCTrajectnummer wordt gehasht tot pseudo DBCTrajectnummer. Het origineel wordt verwijderd en niet aangeleverd.
Meting[68]		
totaalscoreMeting		
gebruiktMeetinstrument		
typeRespondent		
aardMeting		
Typemeting		
Datum		
Item[69]		
Score (0)		
itemnummer(0)		
Argus gegevens worden toegevoegd aan bovenstaande gegevens		
Argus_Opname		
einddatumOpname		
startdatumOpname		
Argus_episode		
Locatiecode		
jurisdischKader		
MateVerzet		
TypeMaatregel		
einddatumtijdEpisode		
startdatumtijdEpisode		
Argus_JuridischeStatus		
JuridischeStatusCode		
einddatumJuridischeStatus		

[68] Er kunnen meerdere metingen plaatsvinden per DBC-traject
[69] Er kunnen meerdere items worden opgegeven per meting.

startdatumJuridischeStatus		

2. Gegevens SBG zoals beschikbaar in de DRM

In onderstaande tabel staat de gegevens zoals beschikbaar in de DRM bij SBG, vóór dat deze verwerkt zijn tot SBG-informatie

Gegevens zoals beschikbaar in de DRM bij SBG, **vóór** dat deze verwerkt zijn tot SBG-informatie	
Zorgaanbieder:	
Zorgaanbiedernaam	
Zorgaanbiedercode	
Patiënt:	
pseudo[pseudoBSN]	
Opleidingsniveau	
Leeftijdsituatie	
[geboortelandMoeder (o)]TRES De herkomstcategorie (autochtoon, niet-westers allochtoon en westers allochtoon) is wel bekend bij SBG.	Dit is met TRES versleuteld en niet toegankelijk voor SBG. Het wordt wel door SBG opgeslagen.
[geboortelandVader (o)]TRES De herkomstcategorie (autochtoon, niet-westers allochtoon en westers allochtoon) is wel bekend bij SBG.	Dit is met TRES versleuteld en niet toegankelijk voor SBG. Het wordt wel door SBG opgeslagen.
[geboortelandPatient (o)]TRES De herkomstcategorie (autochtoon, niet-westers allochtoon en westers allochtoon) is wel bekend bij SBG.	Dit is met TRES versleuteld en niet toegankelijk voor SBG. Het wordt wel door SBG opgeslagen.
[postcodegebied(vier cijfers)]TRES SES-waarde Urbanisatiegraad	Dit was het postcodegebied bij de zorgaanbieder, waarvan de vier cijfers met TRES versleuteld zijn. Het wordt wel door SBG opgeslagen.
Geslacht	
Geboortejaar	
pseudo[pseudoKoppelnummer]	
Zorgtraject	
einddatumZorgtraject	
startdatumZorgtraject	
GAFscore	
primaireDiagnoseCode	
Locatiecode (o)	
zorgdomeinCode	
pseudo[pseudoZorgtrajectnummer]	
Nevendiagnose code	
nevendiagnoseCode	
Behandelaar	
Beroep (o)	
Alias (o)	

primairofNeven (0)	
DBCTraject[70]	
redenEindeDBC	
datumLaatsteSessie	
datumEersteSessie	
einddatumDBC	
startdatumDBC	
DBCPrestatieCode	
RedenNonResponseVoormeting	
RedenNonResponseNameting	
pseudo[pseudoDBCTrajectnummer]	
Meting[71]	
totaalscoreMeting	
gebruiktMeetinstrument	
typeRespondent	
aardMeting	
Typemeting	
Datum	
Item[72]	
Score (0)	
itemnummer(0)	
Argus gegevens worden toegevoegd aan bovenstaande gegevens	
Argus_Opname	
einddatumOpname	
startdatumOpname	
Argus_episode	
Locatiecode	
jurisdischKader	
MateVerzet	
TypeMaatregel	
einddatumtijdEpisode	
startdatumtijdEpisode	

[70] Er kunnen meerdere DBC-trajecten per patiënt worden opgegeven
[71] Er kunnen meerdere metingen plaatsvinden per DBC-traject
[72] Er kunnen meerdere items worden opgegeven per meting.