[redacted]
(adres vertrouwelijk)

Aan het bestuur van de Autoriteit Persoonsgegevens
Mr. A. Wolfsen, voorzitter
Postbus 93374
2509 AJ Den Haag

Datum : 24 maart 2017

Onderwerp : verzoek tot handhavend optreden tegen Stichting Benchmark Geestelijke Gezondheidszorg op basis van de Wbp en de Wgbo

Geachte heer Wolfsen,

Naar aanleiding van mijn e-mail aan u d.d. 17 februari 2017 en in aansluiting op het telefoongesprek, d.d. 20 maart 2017 met xxxxxxxxxxxxxxx senior inspecteur bij de Autoriteit Persoonsgegevens, verzoek ik u handhavend op te treden, op basis van de Wet bescherming persoonsgegevens (Wbp) en de Wet op de geneeskundige behandelingsovereenkomst (Wgbo) jegens Trusted Third Party Stichting Benchmark Geestelijke Gezondheidszorg (SBG).

Ik heb bij dezen een persoonlijk belang omdat mijn medische persoonsgegevens zonder mijn toestemming zijn opgenomen in deze databank.

In mijn brieven aan de Stichting Benchmark GGZ van 12 en 20 februari 2017 heb ik aangegeven dat, zonder toestemming van patiënten, medische persoonsgegevens opgenomen en verwerkt worden in de databank van SBG (een informed consent ontbreekt). Ook heb ik aangegeven dat er mogelijk beveiligingsrisico's zijn bij het invoeren en verwerken van uiterst privacygevoelige medische persoonsgegevens, dat deze herleidbaar zijn en dat de invoer en verwerking ervan onrechtmatig is. Stichting Benchmark GGZ heeft mijn herhaald verzoek, om het verzamelen en verwerken van deze persoonsgegevens in haar databank onmiddellijk te staken, niet ingewilligd.

Stichting Benchmark GGZ heeft, in haar brief van 15 februari 2017, aangegeven dat de gegevens in de databank van SBG niet aangemerkt kunnen worden als persoonsgegevens en dat het gevolg daarvan is dat de Wet bescherming persoonsgegevens niet (meer) van toepassing is bij ontvangst. In haar brief van 6 maart 2017 bericht Stichting Benchmark GGZ mij dat ik mijn verzoek aan het verkeerde adres heb gericht en om die reden niet-ontvankelijk is.

Er worden gegevens van ggz-patiënten aangeleverd en uitgewisseld aan de databank van SBG, ten behoeve van de Benchmark Rapportagemodule (BRaM), die te kwalificeren zijn als (medische en bijzondere) persoonsgegevens:

- Op basis van de erkenning van de artikel 29 werkgroep, dat ook gepseudonimiseerde gegevens gekwalificeerd worden als (medische en bijzondere) persoonsgegevens, in verband met onderkende mogelijkheden van herleidbaarheid, waardoor de Wet bescherming persoonsgegevens en medisch beroepsgeheim weer onverkort van toepassing zijn.
- Op basis van het onderzoek, dat de Autoriteit Persoonsgegevens deed op 17 december 2015 naar het DBC-informatie Systeem (DIS) bij de Nederlandse Zorgautoriteit, waarbij de Autoriteit vaststelde dat de data in het DIS door de Autoriteit Persoonsgegevens worden beschouwd als persoonsgegevens. De DIS-databank is vergelijkbaar met de SBG-databank.
- Door het koppelen van meetgegevens aan een DBC-traject. Tevens is een koppeling met DIS en Vektis mogelijk. Dit staat expliciet vermeld op de website van Volksgezondheidenzorg.info.
- Op grond van het gegeven dat elke persoon een min of meer unieke behandelingshistorie heeft, waarbij al snel helder wordt dat het lastig is te voorkomen dat data uit een gepseudonimiseerd record aan een patiënt te linken is.
  Voor zover ik heb kunnen nagaan, worden de volgende patiëntvariabelen opgeslagen en verwerkt in de databank van SBG: het versleutelde BSN, de viercijferige postcode, geboortejaar, leefsituatie, geslacht, etniciteit (niet verplicht), opleidingsniveau, de vragenlijst

die de patiënten invullen, de zogenaamde ROM- en Argusgegevens: w.o. info over seksualiteit, verslaving, paranoia, dwang- en drangmaatregelen, DBC-gegevens zoals prestatiecode. De Argusinformatie is in 2015 toegevoegd aan de databank van de SBG.

- Op basis van het feit dat er, voor zover ik heb kunnen nagaan, geen periodiek onafhankelijk en deskundige audits plaatsvinden, waar vooraf en daarna periodiek vastgesteld wordt dat aan de voorwaarden, zoals voornoemd in uw brief van 10 januari 2006 aan de minister van VWS, kenmerk z2005-0814, is voldaan, waaruit moet blijken dat er geen sprake is van persoonsgegevens, namelijk:

    - Er wordt (vakkundig) gebruik gemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de zorgaanbieder
    - Er zijn technische en organisatorische maatregelen genomen om herhaalhaarheid van de versleuteling ('replay attack') te voorkomen
    - De verwerkte gegeven zijn niet indirect identificerend.

  Op de website van SBG staat vermeld dat er bij SBG continu interne audits zijn op de naleving van werkprocedures en externe (technische) audits op de Benchmark Rapportagemodule (BRaM), hardware en kantoorautomatisering. Ook staat vermeld dat SBG haar kwaliteitssysteem NEN-EN-ISO 9001 (Norm Kwaliteitsmanagementsystemen) is gecertificeerd en dat SBG NEN 7510 (Norm Medische informatica - Informatiebeveiliging in de zorg) volgt.

  In mijn brief aan de directeur van SBG d.d. 20 februari 2017, heb ik aangegeven dat, voor zover mij bekend, er geen externe audits hebben plaatsgevonden op het informatiebeveiligingssysteem die een gecertificeerd informatiebeveiligingssysteem op hebben geleverd, bijvoorbeeld ISO 27001 of NEN 7510 (inclusief NEN 7512 elektronische communicatie in de zorg, NEN 7513 logging en NEN 7521 toegang tot patiëntgegevens)

Bovenstaande in ogenschouw nemend, het feit dat SBG gefinancierd wordt door de zorgverzekeraars, drie bestuursleden van SBG afgevaardigden van zorgverzekeraars zijn, zorgverzekeraars afnemers zijn van de Benchmark Rapportagemodule, er aan zorgverzekeraars gelieerde partijen afnemers zijn, derden afnemers zijn en er onduidelijkheid is of de databank van SBG wel veilig is en gecertificeerd is conform beveiligingsnormen voor informatiesystemen, zoals ISO 27001 en NEN7510, maakt het zeer twijfelachtig of SBG wel aan te merken is als een TTP. De demissionair minister van VWS stelt immers in haar bovenvermelde brief van 10 januari 2006, dat de onafhankelijkheid, deskundigheid en betrouwbaarheid van een TTP boven elke twijfel verheven dient te zijn.

Risico dat afnemers/gebruikers en in het bijzonder zorgverzekeraars (medische/bijzonderde) persoonsgegevens ontvangen

VECOZO en Vektis hebben een connectie met de zorgverzekeraars. De toegangsautorisatie van gebruikers van de BRaM, is geregeld via VECOZO en in de aansluitvoorwaarden van SBG 20161001 staat vermeld dat gegevens periodiek verzonden worden naar Vektis.

VECOZO is in 2002 opgericht door de zorgverzekeraars CZ en VGZ. In het jaarverslag van Vektis 2014 is te lezen dat Zorgverzekeraars Nederland de enige aandeelhouder van de beherend vennoot van Vektis Beheer B.V. is. Vektis werkt samen met datawarehouse Axians. Middels een datawarehouse kunnen koppelingen aangebracht worden tussen verschillende systemen.

De VECOZO-diensten zijn bestemd voor ketenpartijen in de zorg. VECOZO werkt samen met zorgverzekeraars, softwareleveranciers, koepelorganisaties, Zorgverzekeraars Nederland (ZN), Vereniging Nederlandse Gemeenten, het Inlichtingenbureau en andere partijen om de diensten zo gebruiksvriendelijk mogelijk te maken en nieuwe diensten te ontwikkelen. Ruim 37.000 ondernemingen in de zorg zijn bij VECOZO aangesloten. Hierbij merk ik op dat de stichting Inlichtingenbureau het niet zo nauw neemt met de privacy, aangezien er vermeld wordt dat het bureau persoonsgegevens bezit zonder dat burgers hier weet van hebben en dat er gewerkt wordt met (soms) zeer gevoelige persoonsgegevens.
Daarbij wil ik u wijzen op het feit dat de stichting Inlichtingenbureau ook actief is bij het SyRi(Systeem Risico Indexatie), dat plaats vindt op basis van de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI). Door koppelingen van databases van lokale en centrale overheidsinstanties vindt profilering plaats onder de noemer van fraudeopsporing. Problematisch daarbij is ook dat, door het private karakter van de stichting Inlichtingenbureau, controle door de burger op basis van WOB(Wet

Openbaarheid Bestuur)-verzoeken onmogelijk zijn. Dit staat deels ook vermeld in de petitie 'Stop het schenden van de privacy van patiënten in de zorg', die ik op donderdag 19 november 2015 heb aangeboden aan de heer H. van Gerven, lid van de Tweede Kamer voor de Socialistische Partij.

De afnemers van de Benchmark Rapportagemodule uit de databank van SBG zijn: GGZ Nederland, Inspectie voor de Gezondheidszorg, Landelijk Platform GGZ, Ministerie van VWS, Zorgaanbieders, Zorginstituut Nederland, Zorgverzekeraars. In de aansluitvoorwaarden SBG 20161001, staan echter ook nog overige gebruikers vermeld, niet nader gespecificeerd.

Sleutel

In de beschrijving Pseudonimisatieplatform ZorgTTP 2016 (blz 4) is te lezen dat het sleuteldeel enkel kan worden decrypt door ZorgTTP en dat het datadeel enkel door de uiteindelijke ontvanger kan worden decrypt. Bij het DIS is een sleutel verstrekt aan het Centraal Bureau voor de Statistiek (CBS), waarmee het de pseudo-identiteiten alsnog kan identificeren. Onbekend is of aan het CBS, zoals bij het DIS het geval is, een sleutel is verstrekt waarmee het de pseudo-identiteiten alsnog kan identificeren.

Het verzoek tot handhaving wordt volledig gesteund in de beantwoording van Kamervragen van het SP-fractielid Renske Leijten over het verplicht moeten aanleveren van ROM-data aan de SBG.(kenmerk: 1094180-161209-CZ). In het antwoord van de demissionair minister van VWS op de vragen 9 en 10 zegt deze dat pseudonimisering geen anonimiseringsmethode is, maar een beveiligingsmaatregel om privacy-risico's te verkleinen.(gevolg van standpunt artikel-29 werkgroep) De demissionair minister zegt dat voor de verwerking van (dubbel) gepseudonimiseerde gegevens dus een wettelijke grondslag nodig is, op basis van de Wet bescherming persoonsgegevens. Daarbij is het verkrijgen van een expliciete toestemming van de patiënt één van de grondslagen. Ze vervolgt met de opmerking dat, vanwege het feit dat het toestemmingsvereiste de enige wettelijke grondslag is voor ROM, zij in overleg is met partijen en u. Ze wil bezien of nadere wetgeving nodig is.
Door deze opmerkingen is het klip en klaar dat de ROM-verzameling, ook in de ogen van de demissionair minister, wederrechtelijk plaatsvindt.

Tot slot

Er worden onrechtmatig (medische en bijzondere) persoonsgegevens verzameld, verwerkt en uitgewisseld, in verband met het ontbreken van een informed consent, in een databank met een mogelijk beveiligingsrisico. In verband met pseudonimisatie zijn de gegevens door middel van slimme koppelingen herleidbaar waardoor de privacy van patiënten wordt geschonden.

Nu SBG, in haar eerder vermelde brieven aan mij, d.d. 20 februari en 6 maart, heeft aangegeven dat de Wet bescherming persoonsgegevens niet van toepassing is op de gegevens in haar databank, verzoek ik u nu handhavend op te treden jegens de SBG inzake het schenden van de privacy van patiënten en het niet naleven van de Wbp en Wgbo. Ik vermeld expliciet 'nu' omdat tijdens de rechtszaken UTR 16/3326 WBP V97 en UTR 16/4199 WBP V93, die plaatsvonden op 10 maart 2017 tegen de Autoriteit Persoonsgegevens, duidelijk werd dat de Autoriteit niet handhavend heeft opgetreden jegens Zorgverzekeraars Nederland en de Nederlandse Zorgautoriteit bij eerdere wederrechtelijke levering van datasets aan het ministerie van VWS en het Centraal Planbureau.
De rechter, mr. Verburg, sprak zijn bevreemding uit over het niet doen plaatsen van controle-software in de systemen van de Nederlandse Zorgautoriteit na het duidelijk worden van de wederrechtelijke dataleveranties.

Ik verzoek u, 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.

Ik vraag u om binnen de wettelijke termijn van acht weken een besluit te nemen over dit verzoek om handhaving. Daarmee voorkomt u dat ik een beroep zal doen op de Wet dwangsom en beroep bij niet tijdig beslissen.

Met vriendelijke groet,