Report in response to

research

data processing SBG

Final report

Table of contents

Target research

Course of the investigation

The enforcement request

Purpose, activity and tasks SBG

Information flows and working method SBG

Facts

Background SBG

3.1.1

3.1.2

Current state of affairs SBG

Akwa

3.3.1

3.3.2 Working method Akwa

Purpose, activities and tasks Akwa

Introduction

Direct traceability

Judgement

Research questions

Does SBG process (special) personal data?

4.2.1

4.2.2

4.2.3 Method of anonymization by SBG and indirect traceability

4.2.4

4.2.5

4.2.6

Is SBG the controller?

Resume

Introduction

For some time now there has been discussion about the use of Routine Outcome Monitoring 1 (ROM) as a measuring instrument for the quality of care in Mental Health Care (GGZ) and whether these data are too qualify as personal data within the meaning of the former Personal Data Protection Act (Wbp) and now the General Data Protection Regulation (GDPR).

In that regard, the Dutch Data Protection Authority (AP) has received an enforcement request2 in which it is requested to take enforcement action against the Benchmark GGZ Foundation (SBG). SBG was founded to meet ROM data to make the quality of care in mental health care transparent and measurable, for example by means of benchmarking, so that healthcare providers could learn from this and improve the quality of care.

According to the applicant, the aforementioned ROM data are personal data and, now SBG ROM data and with it according to the applicant, processed personal data without a legal basis (because without her consent), it has requested the AP to allow the collection and processing of data by SBG cease, to have the entire database removed and to monitor any new unlawful filling.

Research

The AP has conducted an investigation into the enforcement request. The research has particularly aimed at the question of whether SBG processes personal data. After all, the answer to this question determines the further course of the investigation. To answer this question, one had to be insightful and understand which data was supplied to SBG. To this end, it was important all the steps of it data delivery process from patient up to and including the processing of the relevant data by SBG and to involve the parties involved and agreements made in that context and to test them against the relevant ones laws and regulations.

During the investigation it became known that SBG would cease its activities and a large part of its activities and the data collected and processed by it to Alliance Quality in the mental health care (Akwa). This prompted the AP to also investigate the data that would still be kept by SBG and would be transferred to Akwa.

Conclusions

The AP comes to the conclusion that the data that SBG has received from healthcare providers (via ZorgTTP) is a processing of personal data about health within the meaning of Article 4, parts 1 and 15, GDPR. The AP also concludes that SBG cannot invoke one of the statutory grounds for exception which could lift the ban on processing health data. This has the consequence that it is prohibited for SBG pursuant to Article 9, paragraph 1, of the GDPR to use the dataset containing process personal data about health.

1 Routine outcome monitoring (abbreviated as 'ROM') is the methodology in mental health care that involves regular measurements of the condition of the clients with a view to evaluation and possible adjustment of the treatment. This goes through filling out questionnaires by the patient.

2 Called a complaint in AVG terminology.

3

1. Background and course of the investigation

1.1

Cause

The reason for the investigation is an enforcement request dated 24 March 2017 in which the AP was requested to take enforcement action against SBG because of the - without permission - collecting and processing of (medical and special) personal data by SBG.

The enforcement request requests the collection and processing of (medical and special) to suspend personal data in the database of SBG as soon as possible and to monitor the immediate destruction of the data in the SBG database. Supervision should also take place renewed illegal filling of the database.

1.2 Purpose of research

1.3

The purpose of the investigation is to determine whether SBG processes personal data and whether this processing is carried

out

complies with the GDPR. The research focuses on the processing that consists of the

receipt and storage of the data by SBG. The AP has investigated whether SBG thus personal data

received and whether these personal data relate to the health of those involved.

Subsequently, the AP investigated whether SBG can rely on a legal ground for exception to the

prohibition of processing of personal data relating to health. Finally, the AP has

investigated whether the dataset that SBG transferred to Akwa is personal data.

Course of the investigation3

The AP has informed SBG of the enforcement request. SBG has on April 24, 2017 on the

application for enforcement and, if requested, provided further information by letter dated 25 August 2017

information to the AP.

The data processing by SBG, as at issue in this enforcement request, is earlier

been the subject of civil proceedings. On August 2, 2017, a judgment in preliminary relief proceedings

rendered4 whereby the court ruled that it had not become sufficiently plausible that the

processing of personal data within the meaning of the Directive5 and the Wbp.

On July 11, 2018, the AP had a conversation with SBG in which SBG explained that in the near future

In the future, data will only be processed with the consent of the patient. That processing would

must be carried out by an independent quality institute.

On December 3, 2018, following a notice of default from the applicant, the AP decided on the

enforcement request. The enforcement request was rejected by this decision because the investigation into that

3 A brief description of the research follows. The more detailed process is included as Appendix 1 to this report.

4 ECLI:NL:RBMNE:2017:4011

5 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and

on the free movement of such data

had not yet been completed at the time and therefore there was no possibility for the AP to take enforcement action

to act. On 10 January 2019, the applicant lodged a pro forma objection against the aforementioned decision.

The AP was informed by SBG on November 27, 2018 by letter that SBG will cease to exist and that

Akwa will take over the role of SBG. In response to this, Akwa and SBG, on 16

January and February 6, 2019 provided additional information to the AP.

5

2. The enforcement request

The enforcement request contains a number of grounds on the basis of which the AP is requested to take enforcement action

to act. These are summarized below.

Grounds for enforcement request

The applicant states that SBG processes her medical data without her consent. These data are

according to the applicant, to be regarded as (medical and special) personal data. With that, according to

the applicant is involved in an unlawful processing of her personal data. She points to the

traceability of the relevant data to individuals, also insofar as it concerns

pseudo-dominant data. According to the applicant, the minister took this position at the time

endorsed.

In addition, the applicant makes a comparison between the SBG database and the DBC information system

(DIS) of the Dutch Healthcare Authority, of which the AP has ruled that the data contained therein

are personal data. Because with the DIS6, CBS has the option to collect data

decryption, she wonders whether Statistics Netherlands also has the opportunity to do so at ZorgTTP. The applicant points

also on a possible link of the SBG measurement data to a DBC trajectory or via a link with

DIS and Vektis, as a result of which (indirect) identification is possible, according to the applicant.

The applicant also argues that it is unclear whether the SBG database is safe and certified

complies with security standards for information systems and doubts them - given the

financing structure of SBG and the participation of health insurers in SBG - equally whether SBG is

is a Trusted Third Party (TTP).

With reference to the connection conditions SBG 20161001, the applicant indicates that the BRaM

reports (Benchmark Reporting Module) can be linked to databases and systems other organisations. In particular, she points to the connections of VECOZO and Vektis with health insurance companies and other organizations. As a result, (medical/special) personal data can be processed.

Request

According to the applicant, the above means that there is a violation of the Wbp and the Law on the medical treatment contract (Wgbo). That is why she requests the AP to collect and processing of (medical and special) personal data in the database of SBG, as soon as possible and to ensure the immediate destruction of the data in the SBG database. Also serves according to the applicant, supervision should be carried out on any new illegal filling of the database.

6 DIS stands for Diagnosis Information System. Information on diagnoses of patients in hospital care, mental healthcare and forensic care ends up in DIS and is managed by the Dutch Healthcare Authority. Also see: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-nza-mag-diagnosedata-uit-dis-limited-verstrekking

3. Facts

The enforcement request first of all raises the question of whether SBG has and processes personal data or processed within the meaning of the Wbp and the GDPR. It is important to answer that question first to provide insight into the relevant information flows; who processes which data? On that will be discussed in this chapter. Among other things, the function that SBG fulfills is discussed, the type data obtained by SBG and from whom SBG receives that data, as well as in what way data is received and processed and then passed on by SBG. Because SBG will cease to exist and Akwa will take over its role and with it the data from SBG - in edited form - has been handed over, the role of Akwa is also briefly discussed. In the assessment of it enforcement request that will follow after this chapter will refer to the one described here information flows.

3.1 Background SBG

3.1.1 Purpose, activities and tasks SBG

There is a legal obligation7 for care providers in the mental health care sector, among others, to provide
good quality care. Zorginstituut Nederland is designated by law8 to take care of the
collect, aggregate and make available information about the quality of care provided.
Healthcare providers are legally obliged to report this information to the Zorginstituut.9 Om aan
To meet this obligation, among other things, SBG was founded by stakeholders under the supervision of VWS
(including GGZ Nederland and Zorgverzekeraars Nederland).
According to article 3 of its articles of association10, SBG aims as a “Trusted Third Party” to support the spiritual
health care (GGZ) to benchmark independently and reliably in the field of treatment effect
and customer satisfaction, thereby making an important contribution through greater transparency
learning and research by professionals and institutions and a quality-enhancing effect for the
to reach the entire GGZ.11
SBG has stated that it achieves this objective through four activities, namely: (1)
SBG has been instructed by the affiliated healthcare providers to carry out the legally required performance
provide indicators (“measuring instruments”) to their supervisor, the National Health Care Institute;
(2) SBG receives (anonymous) ROM information for benchmarking. This benchmarking takes place
on two levels, namely intra-institution, which allows an institution to carry out internal quality assurance and
extra setting that allows institutions to compare themselves with each other or per region; (3) To SBG is through
healthcare providers outsource the storage of a limited set of encrypted data so that it can be made available
be made for scientific research; (4) SBG received the request from GGZ in 2015
Netherlands to also realize the Argus data collection and reporting for the mental health field.12
7 Article 2 Care Quality Complaints and Disputes Act. This also includes the obligation for healthcare providers to opt out
systematically collect and record data on the quality of care so that the data is available to everyone
are comparable with data from other healthcare providers of the same category, see Article 7 paragraph 2 of the Complaints
Quality Act and
dispute care.

8 Article 66d, first and third paragraph of the Healthcare Insurance Act

9 Article 66d, paragraph 2 of the Healthcare Insurance Act

10 See reply letter SBG of 25 August 2017, p. 10, marginal 38 and appendix 11 p. 3.

11 For further details on the objectives, see the SBG reply letter of 25 August 2017, p. 10 ff.

12 See e.g. reply letter SBG of 25 August 2017, p. 10 ff.

SBG thus makes data from the healthcare sector measurable so that it can be benchmarked in the mental health care sector with the aim of maintaining and improving the quality of care. SBG does this on the basis of data from different health care providers. Mental health care providers have patients complete questionnaires, after which the ROM data are supplied to the ZorgTTP foundation. ZorgTTP, which acts on behalf of the GGZ providers, is an independent third party that provides support for the exchange of data files with potentially privacy-sensitive information. It provides, among other things, technical measures, such as pseudonymization and encryption. SBG receives processed data from ZorgTTP for this purpose.13

The SBG Connection Conditions for Healthcare Providers and the SBG Data Protocol show that a healthcare provider must provide all relevant 'Raw Data' to ZorgTTP monthly, via a secure environment by means of an XML delivery. Whereby the ‘Raw Data’ “should meet the minimum data set formulated technical and substantive description”.14

In order to provide data to SBG, a healthcare provider must therefore use ZorgTTP and conform the Minimum Data Set. This is a requirement set by SBG by means of the Conditions of Connection and Data protocol.

After SBG has obtained the information processed by ZorgTTP, the information is further processed by SBG edits them and makes them available - in the form of so-called BRaM reports health insurers and mental health providers. The data processing by GGZ-providers, ZorgTTP and SBG.

Information flows and working method SBG

The information flows and the processing of the data to SBG and the

how SBG processes the data and then passes it on. The data provision is concise

and schematically represented as follows place15:

3.1.2

Data transfer mental healthcare providers

Patients in mental health care provide personal data to their mental health care providers, whether or not via completed

questionnaires. A first pseudonymization step takes place in the Privacy and Sending Module (PVM)

of SBG on location at the mental health care provider. The generated data must comply with the

specifications of the minimum dataset (MDS).16 Only if they meet this delivery standard

they are received by SBG. In the document “SBG Minimum Dataset Data Delivery Standard”17

13 See: https://www.zorgttp.nl/. See also reply letter SBG dated 25 August 2017, p. 32, marginal number 130 et seq.

14 See reply letter SBG of 25 August 2017, appendix 7, p.6 margin number 5.

15 See also reply letter SBG of 25 August 2017, appendix 8, p. 4 through 7.

16 The set of variables as agreed by GGZ Nederland and Zorgverzekeraars Nederland, which describes which (mandatory)

content information must be provided. These variables are listed in the first column of the table as included

in Annex 2 to this report. See also appendix 27 to the SBG reply letter dated 25 August 2017.

17 See reply letter SBG of 25 August 2017, appendix 9.

describes which data must be included in the MDS. There are 29 mandatory ones

data categories that are entered per patient.18 A so-called XSD19 is used to

check whether the information actually meets the requirements of the MDS. This leaves alone

data that meet the requirements of the MDS, the healthcare provider's environment.

Operations within PVM

The PVM performs a number of operations on the entered data. Four of the 29 data categories

be hashed.20 This is the BSN, a link number, a care program number and a DBC

route number. A pseudonym is created for these four data by means of hashing. The

other 25 data categories are not edited.

This splits the file into a pseudonymous part, also known as a key part

and a part with substantive data, also known as data part. Becoming the key part and data part

encrypted in such a way that only the key part is visible to ZorgTTP. The data part with content data

is encrypted so that it is not accessible to ZorgTTP. SBG can decrypt the data part and

so understand, after all, SBG considers this data necessary for making the BRaM reports. Attached

2 this report includes a table of the above data flow and the applied processing.

Data transfer ZorgTTP

After processing in the PVM, the data is transferred to ZorgTTP. This is done via a TLS

(Transport Layer Security) secure connection. This connection ensures the data flow

that is sent between the user and a website or between systems, is encrypted and so on

is made illegible to third parties. The encrypted files are automatically sent to

the Central Module TTP (CMT) of ZorgTTP. The encrypted key part and data part are received

by the Central Module TTP (CMT) at ZorgTTP. Only the CMT of ZorgTTP has the

key to decrypt the key part. The table below makes this clear:

key part

Data part

pseudoBSN

pseudoCouple number

pseudoCare trajectory number

pseudoDBCTroute number

Encrypted and not visible to ZorgTTP and is also

not adjusted by ZorgTTP.

18 This excludes Argus data and follows from the MDS. Argus data is a national dataset for registration of persons with

disabilities

interventions, see also reply letter SBG of 25 August 2017, p. 16 and 17.

19 XSD stands for XML Schema Definition and describes the structure of an XML document. Data entered in the XML

document

can be checked for specific properties in this way. For example, a date in format dd-mm-yyyy, where

19-04-2018 is accepted, but 19-4-18 is not.

20 Hashing is a scrambling or mutation of data using a mathematical function known as a hash

called function. A hash function has the following properties:

-

-

-

-

The result always has the same fixed size regardless of the input.

It is not possible to obtain the input based on the result. A hash function therefore only works in one direction.

The same input always leads to exactly the same result. The smallest change (1-bit) leads to a completely different outcome.

Hash functions are not necessarily secret and accessible and useable for everyone.

It is therefore possible to calculate the output for predictable or frequent inputs. This is a link

between the input and the corresponding output. This is called a link table. In a link table the result can be

searched and the corresponding input.

9

TRES part21 (not accessible to SBG)

[zip code area(four digits)]TRES

[country of birthPatient (o)]TRES

[country of birthFather (o)]TRES

[country of birthMother (o)]TRES

Subsequently, the pseudonyms (the hashed values from the PVM, see previous step) are used in this part

a second pseudonymisation step has been carried out by ZorgTTP. This is used

Advanced Encryption Standard (AES). AES is a symmetric encryption22 algorithm. In contrast

to hash functions, a key is used to encrypt data and

decrypt. This means that the result can be converted back to the input by using

make the same key.

For the pseudonyms received by ZorgTTP, this means the following:

- The pseudonym, the hash value, is encrypted with a key and converted into a

other value. This encrypted value can therefore be seen (for SBG) as a

pseudonym of the pseudonym.

- ZorgTTP keeps the used key to itself and never shares it with SBG. If ZorgTTP this

share the key, then SBG could decrypt the encrypted pseudonym.

- ZorgTTP uses the same key every time to encrypt the pseudonyms. Should

same pseudonym are provided, this will also lead to the same encrypted

value.

- ZorgTTP has the key and can decrypt the encrypted values into pseudonyms (de

hashes from the healthcare provider).

For SBG this means the following:

- Because SBG does not have the key of ZorgTTP, SBG cannot use the pseudonym of the pseudonym

back (decryption) to the pseudonym as known in the PVM at the healthcare provider.

- It is not (just) possible for SBG to make a link table. Cooperation would be required for this

are required by ZorgTTP or the healthcare provider.

- It remains possible for SBG to use data with the same pseudonym (and therefore belonging to

the same person) with previously supplied data. SBG says the following about this:

“To be able to provide ROM information about the course of a treatment (which lasts longer than 3 months on average).

enrichment (with the aim of comparing them), delivery at individual level is therefore necessary. With the modern

one-way pseudonymization technique makes it possible to use the same pseudonym for the same patient without a key

to give.”23

After the second pseudonymization step, the data for ZorgTTP look like this:

key part

Data part

pseudo[pseudoBSN]

21 These data are encrypted by the TRES encryption offered by ZorgTTP, whereby SBG does not have access to the data but see aggregated information about it. See reply letter SBG dated 25 August 2017, p. 50.

22 Symmetric encryption means that the same key is used for encryption and decryption.

23 See reply letter SBG of 25 August 2017, p. 55, marginal number 231.

pseudo[pseudoCouple number]

Encrypted and not visible to ZorgTTP and is also

not adjusted by ZorgTTP.

pseudo[pseudoCare trajectory number]

pseudo[pseudoDBCTroute number]

TRES part (not accessible to SBG)

[zip code area(four digits)]TRES

[country of birthPatient (o)]TRES

[country of birthFather (o)]TRES

[country of birthMother (o)]TRES

Subsequently, the key part and data part are prepared and collected by SBG via the Data Retour Module (DRM).

Data processing by SBG

In the DRM, the key part and data part are decrypted. So the key part consists of the hashed (in PVM) and then encrypted (by ZorgTTP) versions of the BSN, link number, care process number and DBCTroute number. The data part consists of the original data (25 data categories) that are known of a data subject from a mental health care provider. This is described in Annex 2 to this report made clear from a table.

The data is collected by SBG in a database and then further processed. The final

results are presented by SBG in the BRaM.24 BRaM allows for practical variation

treatment outcomes are assessed. Results can be achieved with BRaM at different levels

made visible within mental health care: the average result achieved throughout the Netherlands

(the "SBG Benchmark"), the result of a healthcare provider, the results of the various locations of

that organisation, the results of the various departments per location and the results of the

different practitioners per department.

3.2 Current state of affairs SBG25

As noted, SBG will cease to exist and its role will be taken over by Akwa. In that

In this context, SBG was gradually phased out and dismantled in 2018.

There has been an increasingly limited supply of data by healthcare providers and the

number of SBG employees has fallen sharply. The last employee of SBG is out on May 31, 2019

entered service. SBG only has a liquidator who takes care of the liquidation.

At the moment, no more data is provided to SBG by healthcare providers. SBG has that

the connection conditions have been unilaterally terminated and the healthcare providers and health insurers are happy about

this

December 2018 informed in writing. The last data deliveries to SBG took place at the end of November

and at the end of December 2018. SBG has stated that it no longer has access to data that

provided to SBG by ZorgTTP. Moreover, SBG no longer has access to data that is at least

formed the basis for the BRaM reports. The database that SBG has in the past

built up has already been destroyed and so are backup files of the database.26

24 For further details, see reply letter SBG of 25 August 2017, p. 24 ff.

25 See reply letter to SBG of 16 January 2019 and the opinion of SBG of 27 June 2019.

26 E-mail of 30 April 2019 from Kneppelhout & Korthals N.V. to the AP.

3.3 Akwa

3.3.1 Purpose, activities and tasks Akwa

In Akwa - established on June 1, 2018 - the activities of SBG are (partially) accommodated and continued. The infrastructure for supplying data to SBG is hereby transferred to Akwa. In addition, SBG's dataset is transferred to Akwa in an 'impaired' form27. This impoverishment consists of aggregating three variables and removing ten variables. Below explains exactly what this means in relation to the SBG dataset.

The three categories that are aggregated are:

- Year of birth, but only for people over 80 years old. Only that group gets the same year of birth. Anyone under the age of 80 will not be aggregated and transferred to Akwa.
- Living situation goes from 8 to 5 different options.
- Reason at the end of DBC going from 22 categories to a binary (two possibilities) option.

The following ten categories will be removed:28

- The pseudoBSN. SBG has indicated that following the patient is becoming more difficult because it cannot be tracked across healthcare providers. The pseudoBSN remains the same as you undergo treatment at institutions A and B.
- Zip code area: “The encrypted four digits of the zip code will not be transferred. The derivative SES and degree of urbanization are transferred.” The encrypted four digits are TRES encrypted and were already inaccessible to SBG. SBG already had the SES and degree of urbanization. There therefore does not change anything compared to the SBG dataset with regard to this category.
- Patient's country of birth and derived categories (Native Dutch, Non-Western immigrant and western immigrant) thereof. These categories were not required to be submitted and are optional in MDS.
- Country of birth father and derived categories (Native Dutch, Non-Western immigrant and Western immigrant) thereof. These categories were not required to be submitted and are optional MDS.
- Mother's country of birth and derived categories (Native Dutch, Non-Western immigrant and western immigrant) thereof. These categories were not required to be submitted and are

optional in MDS.

- Reason for non-response for measurement.

- Reason for non-response after measurement.

- Earth measurement

- Type of respondent. SBG says about this; “this is not given for the domains of children and youth and dyslexia transferred. Since the entry into force of the Youth Act, this is no longer provided.”

- Argus data:29 “the data delivery has barely started, so transferring this data is not meaningful. Moreover, Akwa GGZ has no assignment to carry out the Argus registration. Historic comparisons by means of BRaM reports will therefore no longer be possible in the future.”

27 See reply letter from SBG dated 16 January 2019. p. 9 and 10.

28 See reply letter SBG of 16 January 2019, p. 8 and 9.

29 Argus is a minimal data set for the collection of data on the application of the most common freedom-restricting interventions in mental health care.

Of these ten categories, one was thus not accessible to SBG and three were optional could be supplied. This means that of the 25 mandatory data points that were supplied to SBG, 19 data points have been transferred to Akwa. Akwa has the following goal with the dataset eyes: enabling historical comparisons in terms of treatment outcomes and generate patient experiences and associated reports.30 In addition, Akwa will independently collect new data for benchmarking.

3.3.2 Working method Akwa

Akwa has indicated that it will agree with the GGZ provider that the GGZ provider will the patient will be asked for explicit consent for the processing of his/her facts. This agreement will be part of the agreement between Akwa and the mental health care providers. The this choice was prompted by the discussions and problems surrounding SBG and the processing of ROM data has occurred and occurs, not because Akwa believes that the data

that she will receive from the mental healthcare providers are personal data.

The process of supplying data to Akwa will follow the same structure as that

was used for data collection by SBG. Please refer to what has been said about this in

section 3.1.31

30 See reply letter SBG of 16 January 2019, p. 9 and 10.

31 For a further explanation of Akwa's role and working method, see Akwa's reply letter of 16 January 2019.

4. Assessment

4.1 Research Questions

The key question to be answered in the present case is whether the data is true

enforcement request is aimed at qualifying as personal data. Only if that is the case can the AP

assess whether the processing of personal data by SBG is in line with the GDPR. This is where the AP goes

assumes that - in view of the letter of 19 May 2017 submitted by her from her practitioner - data

of the applicant have arrived at SBG according to the (processing) process described in chapter 3.

During the investigation, the AP asked itself the following questions:

-

Is the receipt of data by SBG a processing of personal data? If yes, there is

personal data concerning health?

Is SBG the controller for this processing?

-

- Can SBG invoke a legal exception to the prohibition of processing

personal data concerning health?

It is also important which law applies; the Wbp or the GDPR. At the time of request

enforcement of 24 March 2017, the Wbp applied. The Wbp, which formed the implementation of a guideline

95/46/EG32, however, has been withdrawn on 25 May 201833 and replaced by the AVG34 and the UAVG.35 The AP

tests against the law that is currently applicable, which is the GDPR. However, it is noted that the for

relevant concepts in the AVG compared to the Wbp are virtually unchanged during this study
stayed. The AP is therefore of the opinion that the material assessment under the GDPR is no different from under
the Wbp.

4.2 Processes SBG (special) personal data

4.2.1
Introduction

To answer the question whether SBG processes special personal data, the AP will first check whether
the data processed by SBG qualifies as personal data, i.e. information about a
identified or identifiable natural person (the latter may be directly or indirectly
identified). This means that natural persons should be directly or indirectly traceable
in the SBG dataset. If personal data is involved, it will then be examined whether the
personal data can be qualified as personal data concerning health. Finally, the
AP check whether there is a 'processing' of personal data.

4.2.2 Direct traceability

Article 4, part 1, of the GDPR defines as personal data: 'any information about a
identified or identifiable natural person (“the data subject”). If becomes identifiable

32 Directive of the European Parliament and of the Council of 24 October 1995, Official Journal of the European Communities,
23
November 1995, No. L 281/31 (the so-called Privacy Directive).

33 In Article 51 of the General Data Protection Regulation Implementation Act (UAVG) – which came into effect on
of 25 May 2018 – states that the Wbp will be withdrawn.

34 Article 99, second paragraph, of the GDPR stipulates that the GDPR applies from 25 May 2018.

35 By Royal Decree of 16 May 2018 (Staatsblad 2018, 145) the time for determining the entry into force of the UAVG is
adopted on 25 May 2018. This decision is based on Article 53 of the UAVG, whereby the entry into force of the UAVG on a
time to be determined by Royal Decree has been made possible.

considered a natural person who can be identified, directly or indirectly, in particular to the using an identifier such as a name, an identification number, location data, an online identifier or of one or more elements characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person."

Among other things, the definition makes a distinction between direct and indirect traceability. After this will be therefore first checked whether the data of SBG can be directly traced back to a natural person and subsequently or possibly there is indirect traceability.

As already mentioned in section 3.1, healthcare providers provide data to SBG via ZorgTTP. SBG retrieves this data from ZorgTTP via the Data Return Module (DRM). This data consists of a key part and a data part. The key part consists of the hashed (in PVM) and then encrypted (by ZorgTTP) versions of the BSN, link number, care trajectory number and DBCT trajectory number. It data part consists of the original data (25 data categories) known about a data subject from a health care provider. Examples of this data (which are also listed in full in Annex 2) are gender, year of birth, name of care provider, start and end date of care process.

The AP has determined that the data received by SBG does not contain any data that is direct enable traceability of identified natural persons. In the dataset of SBG namely no data such as the full name, address and/or date of birth of natural persons. Out in the AP's opinion, the foregoing can be concluded in such a way that there is no question of direct traceability.

4.2.3 Method of anonymization by SBG and indirect traceability

Now that the AP is of the opinion that there is no direct traceability, the question then arises to whether there may be indirect traceability through which a natural person becomes identified and, as a result, personal data is involved.

The AP will answer that question on the basis of the provisions of recital 26 in the preamble to the GDPR and recital 26 in the preamble to Directive 95/46/EC. In both considerations indicated that the principles of data protection for any data concerning a

identified or identifiable (natural) person. In addition, it is stated that

these protection principles do not apply to (in short) anonymous data.

After this, the AP will answer the question whether the data that SBG has received concerns anonymous data,

more specifically, whether this data is sufficiently anonymized so that indirect traceability to

stakeholders is no longer possible. In the opinion of the Article 29 Data Protection Working Party on

anonymisation techniques (WP 216 advice 05/2014)36 the question of when

anonymization in such a way that there is no longer any question of indirect traceability.

Risks in the anonymization process

In the Article 29 Data Protection Working Party's previously cited opinion on

anonymisation techniques (WP 216 advice 05/2014)37, the Working Party discusses common mistakes in

pseudonymization. One of the errors mentioned is that removing or replacing one or more

36 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

37 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

attributes38 would lead to an anonymous dataset. In practice, however, it appears that sufficient quasi-

identifiers39, other values or attributes to be present with which a person can become

identified. The Group lists a number of steps by which a dataset can be made anonymous

considered, such as “remove and generalize attributes, remove the original data or at least

merge to a high level of aggregation.”

In the aforementioned opinion on anonymization techniques, the following is stated about a

effective anonymization solution:

“An effective anonymization solution prevents individualization in a dataset, prevents two

records in a dataset (or in two separate datasets) are associated with each other and that from that dataset

information is derived. In general, the removal of directly identifying data is not in itself

sufficient to ensure that the data subject is no longer identifiable. Usually have to go further

measures are taken to prevent identification. Again, this depends on the circumstances and

the purposes of the processing for which the anonymous data are intended." (underlining by AP)

Further on, the opinion discusses three risks that are important in an anonymization process:

-

-

-

traceability, being the ability to individualize a person in the data set by some or all

highlight records;

linkability, being the ability to have at least two records about the same data subject or group

link data subjects (in the same database or in two different databases).

When an attacker can determine (for example, by analyzing the correlation) that two records match a

and the same group of persons are related, without being able to individualize persons within this group,

then the technique passes the 'traceability test', but not the linkability test;

deducibility, being the ability to evaluate the value of a personal characteristic ("attribute") with great

probability from the values of a range of other attributes."

If these risks are sufficiently mitigated or excluded, then the used

anonymization solution "sufficiently resistant to re-identification on the basis of the most probable

and reasonable means used by the controller and any third party."

Risk mitigation for the SBG dataset

When received per record40, the SBG dataset consists of four pseudonymised attributes and 25

normal attributes. As already in section 3.1.2. listed, healthcare providers are required to provide all 29

provide attributes. Looking at this dataset before it's processed into a benchmark, then

the following can be noted about the above risks.

Traceability:

Individualizing a record or person is possible in a number of ways:

- Based on the pseudonymised BSN, a unique record could be extracted from the dataset

become. After all, the pseudonymised BSN is a unique identifier.

38 A personal characteristic. For example, the year of birth, with the corresponding value '2013'. See page 13 of WP29 opinion Opinion 5/2014 on anonymisation techniques.

39 A quasi-identifier is a combination of attributes related to a data subject or group of data subjects. See see page 13 of WP29 Opinion Advice 5/2014 on anonymization techniques.

40 A record is related to one data subject and consists of a series of values for each attribute. See page 13 of WP29 for this opinion opinion 5/2014 on anonymization techniques.

- The combination of the other pseudonymised attributes (couple number, care trajectory number, DBC trajectory number) may be unique enough to create a unique record from the to illuminate the dataset.
- The combination of the other (non-pseudonymized) attributes may also be unique enough to extract a unique record from the dataset.
- The combination of all attributes (both pseudonymized and non-pseudonymized). unique enough to extract a record from the dataset.

Linkability:

According to SBG, it is necessary to study patients over time to draw up the SBG Benchmark Reports track and derive information about the success of a treatment in a particular patient practitioner.41 This makes it necessary to link new information to information already known to SBG about that individual.

Deducibility:

Information such as gender, year of birth and psychological well-being (using the Primary Diagnosis Code and Additional diagnosis code) can be derived per record. In addition, the residential area can be roughly deduced, because information about the healthcare institution is also known.

It is therefore inherent in this way of making benchmarks by SBG, that the risks with with regard to traceability, linkability and deducibility cannot be taken away.

Technical safeguards dataset SBG

In its opinion on anonymization techniques, the Article 29 Data Protection Working Party writes that randomizing and generalizing are two ways in which anonymization can be approached.

Randomization includes a group of techniques “that test the veracity of data modified for the purpose of separating that data from the individual. If the data is sufficiently random (ie say arbitrary or indefinite), it is no longer possible to trace them back to a specific person.”42

Randomization techniques in themselves do not help to reduce the risk of retracement, but they can offer a solution to the risks of deducibility. Examples of such techniques are:

- Addition of noise: attributes in the dataset are changed in such a way that they are less accurate are.
- Permutation: attributes in the dataset are swapped in such a way that they become linked to other stakeholders.
- Differential privacy: a technique that the controller applies to the data queries (queries) made by a specific third party and results in an anonymous dataset, in response to the query. As opposed to releasing the entire dataset.

Generalization refers to the group of anonymization techniques where the attributes of data subjects are generalized or weakened by changing scale or size.

With this, traceability to the person can be ruled out, but further techniques must be applied to counter linkability and deducibility. Examples of generalization techniques:

41 See reply letter SBG of 25 August 2017, appendix 27 about the explanation of the Pseudo-BSN.

42 See page 14 of WP29 Opinion Advice 5/2014 on anonymization techniques.

- K-anonymity: “preventing a data subject from being individualized by combining them with at least k other persons.” For example, generalizing individual dates of birth to year of birth.
- L-diversity and T-similarity: L-diversity says something about the distribution of the attributes within a specific group of persons (equivalence classes). This distribution must be distributed in such a way that it is evenly distributed

to be that an attacker with knowledge of the background of a data subject always has to deal with

with a high degree of uncertainty. T-similarity is a more refined form of this. Finally

should these methods avoid the risk of traceability and deducibility, where

it is no longer possible to trace a person with a probabilistic attack or

specific information about a person.

The documentation received by the AP shows that no use is made of any form of

randomization techniques at the time SBG receives the dataset. With regard to generalizing is

the technique of aggregating (not k-anonymity) was seen, but applied incorrectly. Thus, for example

not the date of birth stored in the dataset, but the year of birth. However, the year of birth is not the

any quasi-identifier. Namely, there are 25 quasi-identifiers, which means there are within the group of

same year of birth individualization is still possible, such as location of healthcare provider, gender,

start date, end date, etc. As a result, properties of k-

anonymity and L-diversity.

In other words, the SBG dataset is detailed to the extent that one or more attributes,

pseudonymised or not, a selection can be made in such a way that one individual is selected from the dataset

can become. As a result, insufficient account has been taken of the risks of traceability,

linkability and deducibility and cannot be about an anonymous dataset.

Pseudonymized data at SBG

The WP 29 Opinion on Anonymization Techniques says the following about pseudonymization:

With pseudonymization, one attribute (which is usually unique) in a record is replaced by another attribute. The

natural person is therefore still indirectly identifiable. Consequently, pseudonymization in itself is not sufficient to establish a

make the dataset completely anonymous.

Pseudonymization reduces the linkability between a dataset and the original identity of a data subject, and

as such is a useful security measure, but not an anonymization method.

The pseudonymization method used by SBG involves a combination of a hash function and encryption

with a secret key. A hash function has “for an input of arbitrary size (a single attribute or

a collection of attributes) has a fixed size output, and cannot be reversed." When encrypted with a secret key "whoever owns the key can easily re-identify each data subject by analyzing the data set decrypt".

The combination of these two methods reduces the risks of rollback or decryption, namely:

- The secret key is known to a trusted third party (ZorgTTP) that does not share it with SBG or any other party. Decoding by SBG is therefore not possible and SBG cannot dispose of it about the hashed versions of the BSN, link number, DBC Route number and Care pathway number.

- The hash function ensures that the trusted third party (ZorgTTP) does not have the original values of the BSN, link number, DBC Trajectory number and Care trajectory number, but only about the hashed versions thereof.
- Due to the combination, it is not possible for SBG to build a link table of all BSNs43 with the associated hashed values.

However, the results of this pseudonymization process are per unique BSN, link number, DBC Trajectory number and Care trajectory number always the same. In other words, every input delivers always exactly the same output. This ensures that new information can be added over time to the information already known at SBG.

The aforementioned risks (traceability, linkability and deducibility) are eliminated with the the current pseudonymization process has not been sufficiently removed. For example, traceability to the person is still possible because the person is now identified by a unique value after pseudonymization. Since the same unique (pseudonymized) values are aggregated over time should be made, the risk of linkability is equally great. Considering the amount of data per pseudonym are stored and the unique combination that results from it remains possible to identify a person identify based on this dataset. The dataset at SBG is therefore a pseudonymised one

data set. The AP considers SBG's position that it does not receive and/or process any personal data as incorrect.44

Conclusion

SBG has insufficient technical guarantees and/or measures on their pseudonymised dataset taken to sufficiently eliminate the risks of traceability, linkability and deducibility to be able to speak of an anonymous dataset. The risk of indirect traceability becomes therefore, with this technical measure, insufficiently removed.

This gives SBG a pseudonymised dataset with personal data that is used for making benchmark reports.

Personal data concerning health

In the previous paragraph, the AP established that the dataset received by SBG contains personal data. In the following question is related to the ban on the processing of personal data about health whether the data that SBG has received is personal data about health.

Article 4(15) of the GDPR provides the following definition of “health data”:

personal data relating to the physical or mental health of a natural person, including data on health services provided with which information is available health status is given

Personal data about health includes all data related to the state of health of a data subject and provide information about the physical or mental past, present and future health status of the person concerned. This can be information about a number, symbol or characteristic assigned to a natural person that uniquely identifies that person

4.2.4

43 The BSN is a predictable series of numbers.

44 See reply letter SBG of 25 August 2017, p. 44 ff.

natural person applies for health purposes and information about, for example, illness, disability,

disease risk or medical history etc.45

The AP has established that the dataset that SBG has received (via ZorgTTP) from healthcare providers contains personal data about health. For example, the dataset contains the name of the healthcare provider and the start and end date of a care process. Healthcare providers also serve the Primary diagnostic code. SBG can place this code next to the code lists that are in the possession of SBG after which the diagnoses, such as depression or borderline, are known for SBG. Also the mere fact that SBG receives data from mental health care providers about those involved, it already indicates that the data is related on health. This data, whether in the form of text or assigned to a natural person figure, thus relates to the mental health of those involved.

The AP has established that the data that SBG has received from healthcare providers (via ZorgTTP) is personal data contains about health within the meaning of Article 4, part 15, GDPR.

Processing

The GDPR applies to the processing of personal data. The AP determines that the receipt and storage of the dataset by SBG is processing within the meaning of Article 4, part 2, GDPR. SBG has this dataset is retrieved and stored via a digital connection at the Data Return Module (DRM). This is an automated process that can therefore be qualified as processing under the GDPR.

Interim conclusion

Based on the above, the AP comes to the conclusion that the data that SBG from healthcare providers receives personal data about health within the meaning of Article 4, parts 1 and 15, GDPR. In addition, the receipt and storage of the dataset by SBG is processing within the meaning of Article 4, part 2, GDPR.

Is SBG the controller?

It has been explained above that the receipt and storage of the dataset by SBG is a processing of personal data. In the context of the question of whether this processing is in line with the GDPR, it is important whether SBG can be regarded as the controller.

Article 4(7) of the GDPR provides the following definition of "controller":

“a natural or legal person, public authority, agency or other body which,

alone or jointly with others, the purposes and means of the processing of personal data

establishes (…)”

By administrative agreement of 2010 it was decided to set up SBG to collect information about

treatment outcomes in mental health care.46 SBG is a foundation consisting of a board, scientific,

user and expert council.47

4.2.5

4.2.6

4.3

45 See GDPR recital 35.

46 See reply letter SBG of 25 August 2017, p. 4.

47 See reply letter SBG of 25 August 2017, appendix 3.

SBG has drawn up various conditions and protocols to achieve its goals.

For example, the preconditions for healthcare providers are laid down in the connection conditions of SBG

must meet in order to use the services of SBG. One of the preconditions is

a data protocol drawn up by SBG. In the data protocol, the nature and specifications of the raw data, it

level to which the raw data relates, the method of delivery as well as the time of delivery and the

minimum required data determined. While healthcare providers are responsible for integrity and

validity of the supplied data, SBG is responsible for the development, management, correct

analyzing and providing the SBG information to healthcare providers and health insurers. SBG has

in addition, the right to have audits carried out on the validity of the data and the integrity of the process

of the delivery. And SBG facilitates healthcare providers in setting up activities,

processes and procedures.48

SBG has also drawn up a quality document. The quality document specifies to which

quality requirements (standards) SBG must meet. For example, SBG has a quality officer and quality cycle established, and audits are carried out on the quality of information security, privacy, the services and realization of SBG information.49 The management of SBG is ultimately responsible for the information security policy that applies to the office environment, employees and data exchange with organizations and individuals.50

SBG uses the data received from healthcare providers not only to make the benchmark but also for the further development and quality improvement of the benchmark reports and the supporting (scientific) research into treatment outcomes in the mental health sector healthcare.51

Based on the above, the AP comes to the conclusion that SBG as controller can be qualified within the meaning of Article 4, part 7, GDPR. After all, SBG generally determines and level of detail which data and how this data is received by SBG. Healthcare providers who do not accept connection conditions of SBG cannot purchase services from SBG. In addition, SBG far-reaching responsibilities and decision-making powers regarding the received dataset, such as validity and its security. This means that SBG can independently make important decisions about the dataset which it receives via ZorgTTP from healthcare providers and therefore as controller is designated.

4.4 Can SBG invoke a legal exception to the prohibition of processing personal data concerning health?

The AP has determined that the data that SBG has received from healthcare providers (via ZorgTTP). contains personal data about health and that SBG is the controller for this.

Pursuant to Article 9(1) of the GDPR, it is in principle prohibited to share health data process. This prohibition does not apply if SBG can invoke a legal ground for exception from Article 9 GDPR jo. Articles 22 to 30 UAVG.

48 See reply letter SBG dated 25 August 2017, appendices 7 and 8.

49 See reply letter SBG of 25 August 2017, appendix 10.

50 See reply letter SBG of 25 August 2017, appendix 20.

51 See reply letter SBG of 25 August 2017, appendix 8.

The AP first of all notes that SBG cannot invoke one of the general grounds for exception
within the meaning of Article 9, second paragraph, GDPR and Articles 22 and 23 UAVG. Insofar as relevant to this research
SBG has not requested explicit permission for the processing from the data subjects, as a result of which
an appeal to Article 9, second paragraph, sub a AVG jo. Article 22, second paragraph, sub a UAVG fails.
SBG cannot successfully invoke the legal ground for exception for scientific or
historical research or statistical purposes within the meaning of Article 9, second paragraph, part j GDPR jo.
article 24 UAVG. It is still unclear whether the processing of health data is necessary
for the purposes of SBG, it is possible to request explicit permission from the
persons involved ex. article 24 sub c UAVG. For example, permission could have been requested from the
involved in completing the questionnaires.
Finally, SBG cannot invoke one of the legal grounds for exceptions regarding data about
health. SBG does not fall under the aforementioned standard addressees of Article 30 UAVG in which this
legal exceptions are arranged. Perhaps unnecessarily, SBG is not an institution or
facility that provides medical care. As a result, SBG cannot invoke Article 9, second paragraph, sub
h GDPR jo. Article 30, third paragraph, sub a UAVG, which stipulates, among other things, that the prohibition on processing of
health data does not apply to care providers, institutions or facilities for
healthcare or social services, insofar as the processing is necessary with it
with a view to proper treatment or care of the person concerned or the management of the person concerned
institution or professional practice.
The AP thus concludes that SBG cannot rely on one of the statutory provisions
grounds for exception that could lift the ban on processing health data.
As a result, it is prohibited for SBG to use the dataset with
process personal data about health therein.

4.5 Other grounds for enforcement request

A number of other arguments have been put forward by the applicant which have not yet been discussed been. The AP explains these arguments below (insofar as they are still relevant) and provides a reaction.

SBG as Trusted Third Party

The applicant doubts whether SBG is a Trusted Third Party (TTP) and points to the financing construction of SBG and the participation of health insurers in SBG.

With regard to this argument, the AP notes the following. Not to mention the manner in which SBG is furnished and financed justifies the conclusion that SBG cannot be regarded as a TTP qualified, the AP notes that given its task as a supervisor of the GDPR and in the past on the Wbp must in this case assess whether SBG processes personal data. Now that the AP believes that SBG processes personal data about health and does not process this data due to the processing ban should have processed, it does not get to the question of whether or not SBG is a TTP. This also applies to doubts raised by the applicant in this context with regard to the security of SBG's systems and the applicable certification.

Key part ZorgTTP

In her enforcement request, the applicant states that she does not know whether Statistics Netherlands has the possibility to do so key part of ZorgTTP to 'decrypt'. In that regard, she indicates that at the Diagnosis Information System (DIS)52 CBS does have a key.

The AP cannot follow the applicant in this reasoning. During the investigation, the AP did not have any evidence has been found that shows that CBS has the ability to collect the key part of Make sure to 'decrypt' TTP. The encrypted key part and data part are received by the Central Module TTP (CMT) at ZorgTTP. Only ZorgTTP's CMT has the key to do this key part to decrypt.

52It concerns Information about diagnoses of patients in hospital care, mental health care and forensic care who ends up in DIS. DIS is managed by the Dutch Healthcare Authority. Also see: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-nza-mag-diagnosedata-uit-dis-limited-verstrekking

5. Preview Akwa

5.1 Transferred data is personal data

During the investigation it became known that SBG would cease its activities and a large part of its activities and the data collected and processed by it to Alliance Quality in the mental health care (Akwa). This prompted the AP to also investigate the data transferred by SBG to Akwa. The AP has asked itself the question whether the data transferred to Akwa are personal data within the meaning of the GDPR.

As explained in section 3.3.1, SBG transfers a depleted dataset to Akwa. By record, yes of the 25 mandatory attributes (as indicated in the Minimum dataset), there are 19 transferred to Akwa. These 19 attributes also include the pseudonymised couple number, DBCTroute number and Care trajectory number. So these are three of four pseudonymised attributes, but also the primary diagnostic code.

SBG has indicated that three attributes are aggregated before being transferred to Akwa. These are year of birth, living situation and reason for ending DBC. However, the year of birth becomes alone aggregated for ages over 80 years. Ages younger than 80 are therefore not aggregated transferred. Looking at the age of the Dutch population, about 4.5 % is 80 years or more older.53 The AP therefore seems likely that the amount of records at SBG about people over 80 years is also lower than the number of records younger than 80 years. Aggregate about this specific age category, while the other birth years are left alone, contribute little to nothing coming from a more anonymous dataset. Aggregate from eight to five categories related to the living situation, is not drastic enough for the same reason.

Considering that there are still 19 mandatory categories per record, including the pseudonymised

variants of the couple number, DBC Trajectory number and Care trajectory number, and the insufficient
aggregate the year of birth and living situation; the AP considers that there are insufficient technical measures
have been taken to reduce the risks of traceability, linkability and deducibility. The
The impoverished dataset is thus again not anonymized, but still contains pseudonymised
personal data related to health.

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

6. Conclusion

SBG has processed personal data about health within the meaning of Article 4, parts 1 and 15, of the
AVG, or - before the AVG was applicable - within the meaning of Article 2, preamble and under a, of the
Wbp. This is because the data received by SBG was insufficiently anonymised, which made it
risk of indirect traceability was insufficiently removed. Furthermore, the AP concludes that
SBG could not invoke one of the legal grounds for exception for this processing
could lift the ban on processing health data. This has the effect of
SBG was prohibited from using the dataset containing personal data pursuant to Article 9(1) of the GDPR
process about health.

7. View of SBG

On June 27, 2019, SBG made its view on the report known to the AP. SBG partly responds to
the legal assessments of the report and, in part, the factual inaccuracies and omissions. Below
the AP first of all responds to the factual inaccuracies and omissions stated by SBG. The addition to the
facts did not, incidentally, lead to a different legal assessment. The AP further notes that in the
within the framework of the objection procedure, a complete review will take place, including the grounds/opinion
of SBG are involved.

7.1 Opinion regarding factual inaccuracies and omissions

View of SBG

In general, the entire report lacks a correct representation of the processing activities of

SBG, for example, the distinction between the four different data processing activities of SBG is missing

whole.

Reply AP

The AP has added SBG's statement about its four activities in section 3.1.1.

View of SBG

Section 3.1.1 indicates that SBG was founded by stakeholders under the guidance of VWS, under

more GGZ Nederland and Zorgverzekeraars Nederland. This is correct in itself, but according to SBG it is missing

that at the time also included the National Platform GGz (LPGGz), the umbrella organization of 20 patient and family

organisations

and now MIND, was involved in the establishment of SBG.

Reply AP

The AP does not consider the addition of SBG relevant to the report. As SBG in reply to

questions from the AP of May 30, 2017 on page 1 (footnote 1), there were other 12

parties involved in the establishment of SBG. The AP has therefore used the words “among other things” and

the addition of all these parties has no relevance to the present legal assessment.

View of SBG

In paragraph 3.1.1 of the report it is indicated that BRaM reports to the National Health Care Institute

were provided. In the opinion of SBG, this is incorrect, the Zorginstituut Nederland did not receive a BRaM

reports delivered. BRaM reports were generated exclusively for target 2a and 2b.

Reply AP

The AP has removed Zorginstituut Nederland from the relevant sentence.

View of SBG

In section 3.1.2 of the report, Vektis is included in the figure as a party to which SBG provides data

would have delivered. However, according to SBG, data has never been supplied by SBG to Vektis

occurred. This was the intention as can be read in the Data Protocol under secondary objective 2f

but never materialized. That is why this data flow was included in the data flow map of

June 26, 2017, which is enclosed as appendix 18 to the reply letter of August 25, 2017.

26

Reply AP

The AP has removed Vektis from the image, now that it is not determinative of the present legal

judgement.

View of SBG

In paragraph 3.1.2 in footnote 19 of the report it is noted that it is possible to predict and

common input, calculate the output. This is technically incorrect in SBG's opinion, a

hash can never be calculated in reverse no matter how often (common) an entry is.

There is no traceable pattern that can lead to predictability.

Reply AP

The AP does not follow this view. Footnote 19 does not mention a traceable pattern that

can lead to predictability. Perhaps the footnote clarification is in the wrong context

read. In this respect, the AP notes the following.

The AP agrees that in "normal" cases (ie not using cryptographically weak hash functions

be) a hash function cannot be reversed. In other words, it is not possible to

an output (the hash) and the hash function used, to arrive at the original input. However, if the

input is a predictable pattern (for example, a series of increasing numbers) or common

(e.g. a simple password) then a table of inputs and its hash (the

output) are calculated. Should one have a hash, which is known to be a predictable one

had input (e.g. one number from an ascending sequence of numbers) then one could trivially find all hashes of

rehashing the entire sequence of numbers one by one. Then the hash can be looked up in the

list just calculated and thus the original input has become known. With this process, the

hash function repeated to get the same output and then retrieve the input (op

to search).

View of SBG

Paragraph 3.2 of the report states that SBG only employs one employee who does this
remains until the liquidation is completed. This is incorrect. The last employee of SBG is out on May 31, 2019
entered service. SBG only has a liquidator who takes care of the liquidation.

Reply AP

The AP sent the report to SBG on May 23, 2019. The fact that SBG argues as incorrect has only
occurred after this date. Nevertheless, the AP will add that SBG will only have one more
liquidator has.

View of SBG

The research questions are listed in section 4.1 of the report. The research questions are according to
SBG formulated inaccurately, incompletely and out of order.

Reply AP

The AP does not follow this view. The AP considers the research questions correct and in the correct order
posed. As described in section 4.2, the AP has assessed whether personal data is involved,
personal data concerning health and the concept of processing. The question of which legal
applicable basis must only be stated if there is a processing of

personal data by a controller and after the prohibition on the processing of
special personal data can be lifted.

View of SBG

In a general sense, there is no clear, well-arranged and complete legal assessment framework that the AP as
has taken as a starting point when assessing the data processing activities of SBG and the
role of SBG in this.

Reply AP

The AP does not follow this view. In various sections, such as from section 4.2.2 to and
with 4.4, states on which articles of law, considerations and guidelines it has its findings

based. SBG is of course free to argue what is lacking in this.

View of SBG

In a general sense, one cannot speak of sound and sufficiently substantiated conclusions, certainly not as regards the qualification of SBG as controller and as regards the fact that SBG cannot rely on a legal exception to the prohibition of processing personal data concerning health. Both conclusions are drawn on the basis of only few paragraphs. In addition, there is generally no careful assessment of the SBG arguments put forward and the substantiation of SBG's positions.

Reply AP

As already mentioned above, in the next phase, the AP will agree on a can express a viewpoint on the AP's findings, consider the legal issues put forward views and qualifications.

7.2 Summary of SBG's opinion

General

SBG is of the opinion that the investigation report is incomplete, incorrect legal considerations and conclusions and furthermore that the conclusions included in the research report cannot be supported by the content of the research report.

View of SBG controller

According to SBG, the investigation report does not make a (clear) distinction between the four various data processing activities by SBG.54 While these all require a separate and careful require legal qualification, which is completely absent from the report.

SBG first of all states that it is not a controller for the four data processors activities now that SBG has no specific legal authority, no implied authority and neither

54 The four data processing activities are:

1. SBG has been instructed by the affiliated healthcare providers to provide the legally required performance indicators (‘measuring instruments’) to their supervisor, the National Health Care Institute.

2a. Benchmarking with (anonymous) intra-institutional ROM information, whereby an institution can carry out internal quality assurance

2b. Benchmarking with (anonymous) ROM information extra setting, so that settings can be compared with each other or per regional comparisons

3. Digital safe for scientific research. The storage of this has been outsourced to SBG by the healthcare provider.

4. Realizing an Argus data collection and reports for the mental health field, at the request of GGZ Nederland.

28

has the actual influence to determine the purposes and means of the processing. SBG always has acted under the actual influence of the stakeholders in mental health care and the scientific council and in order from the healthcare provider. SBG thus notes that it is therefore (a delegation of) patients from the Mental health care, care providers and health insurers was/were jointly and in fact broadly and op level of detail determined which data and in what way data entered SBG, in which this was partly prompted by requirements that followed from the legal obligations to supply data to Zorginstituut Nederland and Argus data. It is possible to apply connection conditions nor lead to the qualification of SBG as controller.

The far-reaching responsibilities and decision-making powers regarding the received dataset, with regard to validity and security thereof, were not independently exercised by SBG either. It kept getting actions of SBG, its management and employees, are actually framed by the patients agreements made by the GGZ, care providers and health insurers. Of independent and/or decisive influence of (the management of) SBG on determining the goals of the data processing activities and the means was thus out of the question. If and insofar as the influence of SBG with regard to the inte putting resources in the context of the data processing activities for purpose 2 was greater than that fit in the role of pure processor, there was at most joint processing processing responsibility of the healthcare provider(s) and SBG. In conclusion, SBG is of the opinion that it cannot be qualified as an independent controller. SBG is too qualify as a processor of the healthcare provider. The connection conditions between the healthcare provider and SBG

can be qualified as a processing agreement.

Reply AP

The controller is the person who, alone or jointly with others, determines the purposes and means for the processing of personal data.55 SBG processes, as set out above in this report put, personal data; it receives personal data and makes demands on how it should be supplied and to the operations to be performed. In the opinion of the AP, this is done in such a way (detailed) level that this does not fit the role of a pure processor. That qualifies SBG also not as a processor, but as a controller. That there is in the processing chain next to SBG other (joint56) controllers or exert influence on SBG is also unaffected that SBG is the controller. It appears that SBG is under the responsibility of its board follows from the Data Protocol of SBG, charged with the analysis of the personal data it receives via TTP receives as well as for the development, management and provision of SBG information and related applications to the users.

In light of and in addition to the above, the AP also notes the following. SBG is responsible for the preparation of comparison information for health insurers, patient organizations and healthcare providers. To this end, SBG specifies in detail which information it passes on the individual healthcare providers must be provided via ZorgTTP in order to be able to measure and to benchmarking. On the basis of SBG's Conditions of Connection57, the healthcare provider must pay all monthly

55 Article 4, part 7, of the GDPR.

56 In this context, the AP points out that the Court of Justice of the European Union (CJEU) has confirmed that any joint responsibility for certain data processing does not detract from the individual responsibility of one of the (joint) responsible persons. cf. CJEU, C□131/12 (Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEP)), 13 May 2014, para. 40. Each of the controllers is responsible for all data processing and compliance of the related obligations (Parliamentary Papers II 1997/98, 25 892, no. 3, p. 58).

57 The legal relationship between a healthcare provider and SBG is governed by the “SBG Connection Conditions Healthcare Providers”. The

Connection conditions contain the conditions that the healthcare provider must meet in order to use the services of SBG

29

to provide relevant so-called 'Raw Data' to ZorgTTP. In the Minimum Dataset (MDS) is recorded

which Raw Data healthcare providers must provide to ZorgTTP. The Raw Data relates to

information about the file, the care provider, the patient, the care process, the secondary diagnosis, the

practitioner, the DBC trajectory58, the measurements and the items. In order to give a true and fair view of the

treatment outcomes, the healthcare provider is also obliged to provide information about the number

DBCs within its organization. The SBG Data Protocol also contains instructions for the healthcare provider

what information must be submitted and how. The board of SBG may decide to modify the Data Protocol

change in accordance with the provisions of the articles of association.

The Data Protocol also states which data will be provided to third parties, under which conditions

and for what purposes. In that context, the Data Protocol provides for an assessment by the board of

SBG, in collaboration with the scientific council of SBG. It is therefore SBG that determines where the door is

its analyzed (aggregated) data ends up.

From the above, the AP concludes that SBG does indeed have the purpose of and means for the processing of

personal data and therefore qualifies as a controller.59

Finally, the AP notes that it is not obliged to make a further breakdown per specific

data processing activity. In that context, the AP notes that SBG for the various

data processing activities receives one set of data on which the Conditions of Connection and the

SBG data protocol apply and the personal data are processed accordingly by SBG

incorporated.

View of SBG legal basis and grounds for exception Article 9 GDPR

In addition, SBG states that the AP has failed to investigate which legal bases are applicable

are in the processing activities of SBG. SBG has explained the basis on which the healthcare provider

can invoke, now that according to SBG the healthcare provider is the controller for the

data processing activities and SBG, as a pure processor, the data processing activities

on the basis of the legal basis of the healthcare provider. The healthcare provider can
SBG for the measuring instruments task invoke Article 6, first paragraph, sub c AVG. For the intra setting
benchmarking with ROM, the healthcare provider can invoke article 6, first paragraph, sub b and c AVG.
Furthermore, the healthcare provider can benchmark with ROM for the extra institution based on Article 6,
first paragraph, sub c GDPR and potentially also sub b. With regard to offering the digital safes
for the purpose of scientific research, the healthcare provider can invoke article 6, first paragraph, under b
AVG. Finally, according to SBG, the healthcare provider can maintain the Argus registration
invoke article 6, first paragraph, sub c AVG.
Furthermore, SBG argues that not it, but the healthcare provider is relying on a legal exception to the prohibition
of the processing of personal data relating to health. Assuming that
personal data is involved, according to SBG, the healthcare provider can undertake the measuring instruments task
invoke Article 9, second paragraph, sub i AVG. For intra-institutional benchmarking with ROM, the
healthcare provider invoke Article 9, second paragraph, sub h GDPR in conjunction with Article 30, third paragraph, opening
words and
under sub a UAVG. As for benchmarking the additional setting with ROM, it is possible that the
care provider cannot invoke the legal exception of Article 9, second paragraph, sub h in conjunction
to make. In addition, the Connection Conditions describe the role of SBG as a data broker and contain the preconditions for
the order to be issued by the mental health care provider to ZorgTTP.
58 DBC stands for Diagnosis Treatment Combination
59 It is important to note that even if someone merely determines the means, he can be responsible. The Article 29-
In its aforementioned advice, the working group indicates that only responsibility is involved when determining the means
where that determination concerns the essential aspects of the resources. cf. working group “Article 29”, Opinion 1/2010 on
the terms “controller” and “processor”, p. 17.

Article 30, third paragraph, opening lines and under a UAVG. For storage by the healthcare provider to SBG
data supplied for scientific research in the digital vault may be the basis

according to SBG can be found in Article 9, second paragraph, sub f AVG. Finally, the healthcare provider can keeping the Argus registration can, according to SBG, invoke Article 9, second paragraph, sub i GDPR.

Reply AP

The AP does not follow SBG in its view and notes the following about this. Because SBG to the judgment of the AP qualifies as a controller and not as a processor, it serves independently to be able to fruitfully invoke one of the grounds for exception for the person entrusted to her personal data about health (a special category of personal data).

process. 60 The AP has explained with reasons that SBG cannot do that.

View SBG permission and anonymization

According to SBG, the AP seems to suggest that asking explicit permission from the patient is the only possibility to obtain health data in the context of quality registration(s). allowed to process. The AP seems to (implicitly) adhere to the 'consent or anonymize approach'. This theory assumes that either (explicit) consent is required, or that data is anonymous must be. Now that the AP has de facto set the bar for anonymous so high that it's practically unattainable, here you go automatically with (explicit) permission. According to SBG, this means that there is a black or white approach, without acknowledging the shades of gray in between. It also ignores that asking (explicit) consent in the context of data processing for quality registrations serious disadvantages, as well as that complete anonymization leads to incorrect results. SBG asks the AP for critically review this point of view.

Reply AP

As explained in detail in the report, the AP is of the opinion that there are (special) personal data. This means that SBG may only process that data if it can rely on one of the exceptions. Now that SBG cannot do that, that means the relevant personal data can only be processed with the (explicit) consent of the data subject. That this, like SBG argues, leads to serious disadvantages and incorrect outcomes, is - whatever else it may be - one as a result of the applicable laws and regulations as well as of the choices made in the context of the

setting up and furnishing SBG. However, the AP sees no reason to argue otherwise in this regard
to take a position.

View of SBG personal data

SBG primarily takes the position that it does not process personal data. According to SBG, the door can
the WP29 opinion cited by the AP should not be used as a yardstick for determining whether the data is sufficient
be anonymized. In SBG's opinion, there are two other and interrelated criteria
which must be taken as a starting point when answering the question of whether data is sufficient
are anonymised.

Referring to the Breyer judgment, SBG first of all states that it is no longer possible to speak of
means that can reasonably be expected to be used to protect the natural person
identify if (1) identification is prohibited by law or (2) is impracticable in practice, for example because
it requires an excessive effort so that the risk of identification seems insignificant in reality.
There is then no question of indirectly traceable data and therefore no question of personal data.

60 See article 9 GDPR and articles 22 – 30 UAVG.

Secondly, according to SBG, the 'motivated intruder test' described by the Information is relevant
Commissioner's Office (ICO), the British privacy regulator, in the document "Anonymisation:
managing data protection risk. Code of practice". The relevant question is whether it is for a motivated
intruder, given his knowledge and available resources such as time, money and manpower, reasonably
it is possible to include natural persons in the anonymised data that SBG receives from Stichting ZorgTTP
to identify. According to SBG, the answer to the aforementioned question is negative. Moreover
it is about the possibility of identification and not the possibility of individualization. SBG lightens this
as follows.

SBG is unable to extract the encrypted and encrypted attributes from ZorgTTP on behalf of the
source XML file provided to SBG by the healthcare provider. Now SBG is not considered capable
to decrypt the encrypted and encoded attributes from the Source XML file dat

ZorgTTP, it is also unlikely that a motivated intruder will decrypt this

will be reasonably able. A motivated intruder will require the cooperation of ZorgTTP and the

care provider to come to decryption and identification, which cooperation of course

will be remembered. If the motivated intruder would already have access to the sufficient

anonymised dataset, he is dependent on the use of illegal means, such as hacking or

breaking into the systems of ZorgTTP and/or the healthcare provider in order to decrypt it. The

however, the need to use such illegal means means that this is no longer the case

means of identification that can reasonably be used. That is why, according to SBG, there is no other option than

It can be concluded that the Source XML file that ZorgTTP produces after processing is sufficient

anonymized file, which means that SBG does not receive any personal data.

According to the AP, it is possible for SBG, given the use of the same pseudonym (van het

pseudonym), individualize a person in a dataset. In the opinion of SBG this is correct.

Subsequently, according to SBG, the question arises whether when the possibility of individualization (and therefore

not to identify!) this leads to indirect traceability and thus to the

qualifying personal data. According to SBG, the answer to that question is negative, while the AP

assumes an affirmative answer.

Subsequently, the AP points to three risks mentioned in the opinion that must be taken into account in the

anonymization process, namely the chance of traceability, linkability and deducibility. The AP

concludes after discussing the three risks that SBG does not sufficiently mitigate them. Referring to

de Tekst & Comment 'Privacy and telecommunications law', SBG states, must be the correct criterion

whether it is for a motivated intruder, given his knowledge and available resources such as time, money and

manpower, it is reasonably possible to identify natural persons in the anonymised data

identify. By using the wrong criterion to determine whether there is indirect

traceable data, the AP has not been able to come to the (interim) conclusion that SBG uses personal data

processed.

In addition, SBG also appoints the Minister of Health, Welfare and Sport (“VWS”)

answer to parliamentary questions from member Leijten (SP) on 23 March 2017 answered: “Due to the described process, the ROM data has been processed in such a way that healthcare providers do not have to tell SBG to the person supply information”. SBG is surprised that the AP, when coming to its conclusion that SBG personal data processes this comment from the Minister of Health, Welfare and Sport about the qualification of the apparently rejected data that SBG processes without any discussion.

SBG indicates that it is surprised that the AP accepts the conclusions in the audit reports submitted by SBG apparently rejected without any discussion. It had been in the way of the AP to motivated

to indicate the basis for the apparent rejection of the conclusions in the two audit reports is based.

In 2009, the Dutch Data Protection Authority (“CBP”), the predecessor of AP, in another research report described that the use of pseudonymization in accordance with five conditions leads to sufficiently anonymized data. SBG remarks in this context that it seems that the AP has done this earlier has implicitly (!) abandoned the proposed approach. It is of course possible that there are new insights arise, which means that an old approach can no longer be used as a starting point.

However, it cannot be the case that when answering the question whether SBG processes personal data, a new approach is applied, while SBG was allowed to use it according to the submitted audit reports confidence to meet the conditions that were part of the old approach. This delivers according to SBG, this conflicts with the principle of legal certainty.

Reply AP

The difference of opinion between SBG and the AP focuses essentially on the question of whether there is indirect traceability. The AP believes that this is the case and therefore cannot agree with the view from SBG. This will be explained below.

The similarity that SBG makes with the judgment of the Court of Appeal regarding Breyer is in the opinion of the AP not on. This case only concerns the indirect traceability of dynamic IP addresses. Thereby no additional information available from the online media service provider. This is why it serves

necessarily turn to the Internet Service Provider to resolve the dynamic IP address
to a person. At SBG, however, there is much more to each pseudonymised patient
information available. It is not just one data point, as is the case with the dynamic IP address,
only dozens.61 In view of the type of data and the number of data processed about one patient
over a longer period of time, there is therefore (the risk of) indirect derivation for more parties and the public
sources cannot be avoided. The AP also notes that SBG's choice is based on patients
individualisable in combination with the choice to directly identify personal data
pseudonymization leads to a potentially vulnerable system that poses a real risk of identification
brings. In this context, the AP notes that via a request for access to personal data a
data subject to the healthcare provider and subsequently to SBG in a legitimate manner
to make.

Where SBG refers to the 'motivated intruder test', the AP notes the following. With regard to a
motivated intruder with data from various healthcare providers and who has access to the
raw SBG database (which, as already noted, contains a large amount of data points per pseudonym)
is indirect identification, by means of combining these data and taking into account the
current available technology and the constant and rapid development that the technology undergoes
to be considered very plausible. In addition, the AP emphasizes that SBG is the controller
must also explicitly take into account future situations and developments. they referred
to WP advice 216 05/2014 and recital 26 of the GDPR cited in this report.

SBG also refers to answers from the Minister of Health, Welfare and Sport to
Parliamentary questions and in which the minister concludes that SBG does not have any information that can be traced back
to the person
gets delivered. In this regard, the AP notes that as an independent supervisor, given the
its assigned task, independently and independently assesses whether there is
personal data and this is separate from the opinion that the Minister has and explains in this regard
for example, answers to parliamentary questions.

61 For further details, see Appendix 2 to this report.

33

SBG also refers to the audit reports compiled by external parties. Insofar as the AP with regard to the question whether there is processing of personal data leads to a different conclusion than the to the authors of the audit reports, the AP notes that it has explained in this report with reasons why it believes that there is (a processing of) personal data. The AP opposes that background there is no reason to explicitly refute (the conclusions from) the audit reports.

Finally, SBG refers to a letter from the Dutch DPA from 2009. The AP notes the following about this. If one of the conditions necessary for the conclusion that there is sufficient anonymization data, the letter from the Dutch DPA states that the processed data is not indirectly identifying may be. As explained above with reasons, this is now the case with the data from SBG not really the case. The AP therefore does not see that the conditions stated in the letter from the Dutch DPA are released.

34

Attachment 1

Course of the investigation

In a letter dated 24 March 2017, the applicant requested the AP to take enforcement action against SBG.

The AP then informed SBG of the enforcement request.

In a letter dated 24 April 2017, SBG responded to the enforcement request.

In a letter dated 1 May 2017, the applicant was asked to provide further substantiation of the request.

On May 23, 2017, the AP received the requested substantiation.

In a letter dated 30 May 2017, the AP informed SBG that it would conduct an investigation into the processing of personal data by SBG. In that letter, the AP asked questions to SBG.

The AP also informed the applicant in a letter dated 30 May last about the start of this investigation.

On August 2, 2017, a judgment in summary proceedings was rendered with regard to the present issue, with SBG as defendant.62 The preliminary relief judge ruled that this is not sufficiently plausible

that it concerns the processing of personal data within the meaning of the Directive63 and the Wbp.

In a letter dated 25 August 2017, SBG answered the AP's questions.

On September 11, 2017, the applicant was informed by e-mail that the AP was still working on the assessment of the information received from SBG and the meaning of the judgment in summary proceedings.

In a letter dated 5 February 2018, the applicant expressed her concerns in writing to the AP regarding the supply of medical data by GGZ institutions to SBG, because the applicant had received information from the media learned that a third of the mental health care institutions had gone ahead with this. This is what the applicant saw reason to request the AP to immediately stop the supply of data to SBG pending the investigation to have laid.

By e-mails of 22 and 31 January 2018, 17 February 2018 and 30 March 2018, the applicant sent additional information sent to the AP.

By letter dated 18 April 2018, the applicant declared the AP in default due to the lack of a decision to her enforcement request. On 2 May 2018, the applicant withdrew the notice of default.

On July 11, 2018, the AP had a conversation with SBG in which SBG explained that it would shortly wants to process data only with the consent of the patient. That processing should take place found by an independent quality institute.

On October 4, 2018, SBG informed the AP by e-mail that important decisions had been made regarding the future/discontinuation of SBG.

62 ECLI:NL:RBMNE:2017:4011

63 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

On November 20, 2018, the AP received a written notice of default from the applicant.

On November 27, 2018, the AP was further informed by letter from SBG about the future/discontinuation of SBG.

On December 3, 2018, the AP decided on the enforcement request. The enforcement request is herewith

decision rejected on the grounds that the investigation into SBG had not yet been completed at that time and therefore there was no possibility for the AP to take enforcement action against SBG.

This decision was sent to the applicant and SBG by regular and registered mail on 3 December 2018 and on January 9, 2019 again by regular and registered mail as well as by e-mail on January 8, 2019 to applicant, when it became apparent that the registered post had not been collected.

On 14 December 2018, SBG and Akwa were asked for further information.

On January 16, 2019, Akwa and SBG provided the requested information to the AP.

On 10 January 2019, the applicant lodged a pro forma objection against the AP's decision of 3 December 2018. The AP received this objection on January 11, 2019.

The DPA has granted the applicant a term to supplement its grounds, ending on 13 February 2019.

On 5 February 2018, the applicant stated that it had engaged a lawyer and for that reason requested a four-week extension. The AP granted that request in a letter to the applicant dated 6 February 2019.

By e-mail dated 6 February, 14 March and 30 April 2019, SBG informed the Commission on 16 January 2019 provided additional information upon request.

36

Appendix 2

1. PVM Data Processing

The table64 below contains three columns. The first column describes the data before processing the PVM, second column after the processing by the PVM and the third column what kind of processing occurred. The '(o)' indicates that this data can be supplied optionally. With red indicates which data will be processed into pseudonyms in the PVM and is indicated in blue which data is aggregated and encrypted with TRES. The red part is provided by ZorgTTP referred to as the key part and the other data as the data part.65 The data part is not accessible by ZorgTTP, but for SBG. The key part and data part are encrypted in such a way that only the key part

transparent for ZorgTTP. The substantive data part (shown in black) only becomes clear again

at SBG during the later steps.

Data for processing by PVM66

Data after processing by PVM

Type of processing that has

Without Argus data

Healthcare provider:

Healthcare provider name

Healthcare provider code

Patient:

BSN

occurred

Pseudo BSN

A BSN is hashed into pseudoBSN.

The original BSN will be deleted and

not delivered.

Educational attainment

Age situation

country of birthMother (o)

[country of birthMother (o)]TRES

The country is encrypted with TRES and not

For SBG this is converted into

accessible to SBG. It will be

origin categories: native,

stored by SBG.

non-Western immigrant and Western

immigrant.

country of birthFather (o)

[country of birthFather (o)]TRES

This is TRES encrypted and not

For SBG this is converted into

accessible to SBG. It will be

origin categories: native,

stored by SBG.

64 Compiled from the documents:

- 20170825 - DEF answer questions AP, pages 45 and 46

- Appendix 18 – Flowchart-data-privacy-SBG-V1_9-20170628

- SBG Minimum Dataset, Data delivery standard including Argus delivery, version 20180701

- Factsheet_pseudonymisation_ZorgTTP_2017

- Annex 27 - MDS explanation per variable

65 See Factsheet_pseudonimisatie_ZorgTTP_2017

66 This is based on the MDS, the examples of XML files (SBG Example XML with and without Argus) and the XSD file.

The documents can be found at: https://www.sbggz.nl/Documents under Technical Documentation.

country of birthPatient (o)

[country of birthPatient (o)]TRES

This is TRES encrypted and not

non-Western immigrant and Western

immigrant.

For SBG this is converted into

accessible to SBG. It will be

origin categories: native,

stored by SBG.

non-Western immigrant and Western

immigrant.

Zip code area

[zip code area(four digits)]TRES

“These will be pre-ordered by ZorgTTP

[these are the four digits of the zip code]

Four digits of the postal code are indicated with

reception at SBG TRES encrypted and

TRES encrypted and are not

aggregated to two main ones

insightful for SBG, see step 4b.

casemix variables namely

Degree of urbanization (5 groups) and Social

For SBG, the zip code is converted

Economic Status (5 groups). SBG

to SES value and Urbanization degree.

therefore does not receive a zip code.”

Pseudo Couple Number

A link number is hashed to

pseudopair number. The original

is deleted and not delivered.

Pseudo care pathway number

A care process number is hashed

to pseudocare trajectory number. It

original is deleted and not

supplied.

Sex

Year of birth

Couple number

Care trajectory

end dateCare process

start dateCare process

GAF score

primaryDiagnosticsCode

Location code (o)

caredomainCode

care pathway number

Additional diagnosis code

secondary diagnosisCode

Practitioner

Occupation (0)

Alias (0)

primary or cousins (0)

DBC Trajectory67

reasonEndDBC

67 Multiple DBC trajectories can be specified per patient

dateLastSession

dateFirstSession

end dateDBC

start dateDBC

DBCPerformanceCode

ReasonNonResponsePremeasurement

ReasonNonResponseNameting

DBCTroute number

Pseudo DBCTroute number

A DBCTroute number is hashed

to pseudo DBCTroute number. It

original is deleted and not

supplied.

Measurement68

totalscoreMeasurement

used Measuring instrument

typeRespondent

earth measurement

Type measurement

Date

Item69

rating (0)

item number(0)

Argus data is added to

above data

Argus_Record

end dateRecording

start dateRecording

Argus_episode

Location code

legal framework

MateResistance

Type Measure

end datetimeEpisode

startdatetimeEpisode

Argus_LegalStatus

LegalStatusCode

end dateLegalStatus

68 Multiple measurements can take place per DBC trajectory

69 Multiple items can be specified per measurement.

start dateLegalStatus

2. SBG data as available in the DRM

The table below shows the data as available in the DRM at SBG before it has been processed

to SBG information

Data as available in the DRM at SBG, before being processed into SBG information

Healthcare provider:

Healthcare provider name

Healthcare provider code

Patient:

pseudo[pseudoBSN]

Educational attainment

Age situation

[country of birthMother (o)]TRES

This is encrypted with TRES and not accessible to SBG.

It is, however, stored by SBG.

The category of origin (native Dutch, non-western immigrant

and Western immigrant) is known to SBG.

[country of birthFather (o)]TRES

This is encrypted with TRES and not accessible to SBG.

The category of origin (native Dutch, non-western immigrant

It is, however, stored by SBG.

and Western immigrant) is known to SBG.

[country of birthPatient (o)]TRES

This is encrypted with TRES and not accessible to SBG.

The category of origin (native Dutch, non-western immigrant

It is, however, stored by SBG.

and Western immigrant) is known to SBG.

[zip code area(four digits)]TRES

This was the postal code area at the healthcare provider, of which the

SES value

Urbanization degree

Sex

Year of birth

pseudo[pseudoCouple number]

Care trajectory

end dateCare process

start dateCare process

GAF score

primaryDiagnosticsCode

Location code (o)

caredomainCode

pseudo[pseudoCare trajectory number]

Additional diagnosis code

secondary diagnosisCode

Practitioner

Occupation (0)

Alias (0)

four digits are encrypted with TRES.

It is, however, stored by SBG.

40

primary or cousins (0)

DBC Trajectory70

reasonEndDBC

dateLastSession

dateFirstSession

end dateDBC

start dateDBC

DBCPerformanceCode

ReasonNonResponsePremeasurement

ReasonNonResponseNameting

pseudo[pseudoDBCTroute number]

Measurement71

totalscoreMeasurement

used Measuring instrument

typeRespondent

earth measurement

Type measurement

Date

Item72

rating (0)

item number(0)

Argus data is added to above

facts

Argus_Record

end dateRecording

start dateRecording

Argus_episode

Location code

legal framework

MateResistance

Type Measure

end datetimeEpisode

startdatetimeEpisode

70 Multiple DBC trajectories can be specified per patient

71 Multiple measurements can take place per DBC trajectory

72 Multiple items can be specified per measurement.