Report as a result of

research

data processing SBG

Final report

Index

Summary

1.

1.1

1.2

1.3

2.

3.

3.1

3.2

3.3

4.

4.1

4.2

4.3

4.4

4.5

5.

5.1

6.

Background and course of the investigation

Cause

Purpose of research

Course of the investigation

The enforcement request

Goal, 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

Goal, activities and tasks Akwa

Introduction

Direct traceability

Rating

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 a controller?

Introduction

There has been discussion for some time about the use of Routine Outcome Monitoring 1 (ROM) as a measurement tool for the quality of care in mental health care (GGZ) and whether this data can be 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 is requested to take enforcement action against the Benchmark GGZ (SBG) Foundation. SBG was founded to ROM data to make the quality of care in mental healthcare 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 thus 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 discontinue, to have the entire database removed and to monitor new illegal filling.

Research

The AP conducted an investigation in response to the enforcement request. The research has specifically aimed at whether SBG processes personal data. After all, the answer to this question determines the further course of the investigation. To answer this question, insightful and understand which data has been supplied to SBG. To this end, it was important to follow all the steps of the patient data delivery process up to and including the processing of the relevant data by SBG and involve the parties involved and agreements made in this regard and check them against the relevant laws and regulations.

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

Conclusions

The AP comes to the conclusion that the data that SBG (via ZorgTTP) has received from healthcare providers is processing of personal data relating to health within the meaning of Article 4(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 the processing of health data. This results in it is prohibited for SBG pursuant to Article 9(1) of the GDPR to use the data set containing to process personal data about health.

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

2 Called a complaint in GDPR terminology.

1. Background and course of the investigation

1.1 Cause

The reason for the investigation is an enforcement request of 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 SBG database as soon as possible and to monitor the immediate destruction of the data in the SBG database. Supervision should also take place on 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 in is in accordance 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 provides personal data has received and whether this personal data relates to the health of data subjects.

The AP then examined whether SBG can invoke a legal ground for exception to the prohibition of processing of personal data relating to health. Finally, the AP has investigated whether the data set 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 enforcement request has given its view and, if requested, further details information provided to the AP.

The data processing by SBG, as addressed in this enforcement request, is earlier been the subject of civil proceedings. A judgment in summary proceedings was issued on 2 August 2017 pointed out4 in which the court ruled that it has not become sufficiently plausible that the processing of personal data within the meaning of the Directive5 and the Wbp.

On 11 July 2018, the AP had a conversation with SBG in which it was explained by SBG 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 3 December 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 on that

3 A brief course of the research follows. The more extensive 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 there was therefore 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 letter by SBG on November 27, 2018 that SBG will cease to exist and that

Akwa will take over the role of SBG. As a result, Akwa and SBG asked for 16
provided additional information to the AP on January and 6 February 2019.

2. The enforcement request

The enforcement request contains a number of grounds on the basis of which the AP is requested to enforce on
to act. These are summarized below.

Grounds for enforcement request

The applicant argues that SBG processes its medical data without its consent. This data is
to be regarded as (medical and special) personal data according to the applicant. According to this,
the applicant alleges an unlawful processing of her personal data. She points to the
traceability of the relevant data to individuals, also insofar as it concerns
pseudominized data. According to the applicant, the Minister adopted 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 Statistics Netherlands has the option of collecting data at DIS6
decryption, she wonders whether Statistics Netherlands also has the possibility to do so at ZorgTTP. The applicant points
also on a possible link of the SBG measurement data to a DBC route or via a link with
DIS and Vektis, as a result of which, according to the applicant, (indirect) identification is possible.

The applicant also argues that there is a lack of clarity as to whether the SBG database is safe and certified
conforms to security standards for information systems and doubts them - in view of the
financing construction of SBG and the participation of health insurers in SBG - also whether SBG is
is a Trusted Third Party (TTP).

With reference to the connection conditions SBG 20161001, the applicant states that the BRaM
reports (Benchmark Reporting Module) can be linked to databases and systems of
other organizations. In particular, she points to the connections of VECOZO and Vektis with

health insurers and other organizations. As a result, (medical/special) personal data

can be processed.

Request

According to the applicant, the above means that there has been a violation of the Wbp and the Act on the

medical treatment agreement (Wgbo). That is why she requests the AP to collect and

processing (medical and special) personal data in the SBG database as soon as possible

and to monitor the immediate destruction of the data in the SBG database. Also serves

according to the applicant, supervision should take place on new illegal filling of the database.

6 DIS stands for Diagnosis Information System. Information about 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-providing

3. Facts

The enforcement request first of all raises the question whether SBG has and processes personal data

or processed within the meaning of the Wbp and the AVG. To answer this question it is important to

first to provide insight into the relevant information flows; who processes which data? thereupon

is discussed in this chapter. Among other things, the function that SBG performs, the type of

data that is 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

will cease to exist and Akwa will take over her role, taking SBG's data - in edited form

- has been transferred, the role of Akwa is also briefly discussed. In the assessment of the

enforcement request that will follow after this chapter will be reverted to the described here

information flows.

3.1 Background SBG

3.1.1 Purpose, activities and tasks SBG

There is a legal obligation7 for, among others, healthcare providers in the mental healthcare sector to provide

quality care. The National Health Care Institute is designated by law8 to take care of the
collecting, merging and making available information about the quality of care provided.
Healthcare providers are legally obliged to report this information to the Zorginstituut.9 In order to
among other things, to meet this obligation, under the supervision of VWS, SBG has been established by stakeholders
(including GGZ Nederland and Zorgverzekeraars Nederland).
According to Article 3 of its statutes10, SBG aims as a “Trusted Third Party” to
healthcare (GGZ) independently and reliably benchmark in terms 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
reach the entire mental health care system.11
SBG has stated that it achieves this objective through four activities, namely: (1)
SBG has been instructed by the affiliated healthcare providers to meet the legally required performance
indicators (“measuring instruments”) to be supplied to their supervisor, the National Health Care Institute;
(2) SBG receives (anonymous) ROM information for benchmarking. This benchmarking takes place
on two levels, i.e. intra-institution through which an institution can carry out internal quality assurance and
extra setting allowing institutions to compare themselves with each other or per region; (3) SBG has passed
healthcare providers outsource the storage of a limited set of encrypted data so that it can be made available
be asked for scientific research; (4) SBG received a request from GGZ . in 2015
The Netherlands to also realize the Argus data collection and reporting for the mental health field.12
7 Article 2 Care Complaints and Disputes Act. This also includes the obligation for healthcare providers to
systematically collecting and recording 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
disputes care.
8 Article 66d, paragraphs 1 and 3 of the Health Insurance Act
9 Article 66d, paragraph 2 of the Health Insurance Act

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

11 See more detailed response letter from SBG dated 25 August 2017, p. 10 ff.

12 See, among other things, reply letter SBG of 25 August 2017, p. 10 ff.

SBG thus makes data from the healthcare sector measurable so that benchmarking can be done in the GGZ
with the aim of maintaining and improving the quality of care. SBG does this on the basis of data from
various health care providers. Mental health care providers have patients complete questionnaires, after which the ROM
data are delivered 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.13
It appears from the SBG Connection Conditions for Healthcare Providers and the SBG Data Protocol that a healthcare
provider
must provide all relevant 'Raw Data' to ZorgTTP on a monthly basis, via a secure environment, by
by means of an XML submission. Where the 'Raw Data' "must comply with 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 comply with
the Minimal Data Set. This is a requirement that SBG sets by means of the Connection Conditions 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 healthcare providers. In the following, the data processing by mental health care providers is
discussed in more detail.
providers, ZorgTTP and SBG.
Information flows and working method SBG
In the following, the information flows and the processing of the data to SBG and the

way in which SBG processes the data and then passes it on. The provision of data is succinct and schematically shown as follows place15:

3.1.2

Data transfer GGZ providers

GGZ patients provide their GGZ providers with personal data, whether or not via completed data questionnaires. A first pseudonymization step takes place in the Privacy and Send Module (PVM) from SBG on location at the GGZ provider. The generated data must comply with the specifications of the minimum data set (MDS).16 Only if they comply with this delivery standard can they are received by SBG. In the document “SBG Minimum Dataset Data Delivery Standard”17 it is

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

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

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

16 The set of variables as agreed by GGZ Nederland and Zorgverzekeraars Nederland, which describes which (mandatory) substantive information must be provided. These variables are included in the first column of the table as recorded in Appendix 2 to this report. See also appendix 27 to SBG reply letter dated 25 August 2017.

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

describes which data must be included in the MDS. There are 29 mandatory data categories that are entered per patient.18 A so-called XSD19 is used to verify that the information actually meets the requirements of the MDS. This leaves alone data that meet the requirements of the MDS, the environment of the healthcare provider.

Operations within PVM

The PVM performs a number of operations on the entered data. Four out of 29 data categories be hashed.20 This is the citizen service number (BSN), a link number, a care program number and a DBC track number. For these four data, a pseudonym is created by means of hashing. The other 25 data categories are not edited.

This results in a split of the file into a pseudonymous part, also known as a key part

referred to as a part with content data, also referred to as a data part. The key part and data part become

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 cannot be accessed by ZorgTTP. SBG can decrypt the data part and

so understand, SBG deems 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 HealthcareTTP

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 that 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. In this case, only the ZorgTTP CMT has the

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

key part

data share

pseudoBSN

pseudoLink number

pseudoCare track number

pseudoDBCTraject number

Encrypted and not transparent for 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 freedom-restricting

interventions, see also SBG reply letter 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 the format dd-mm-yyyy, where

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

20 Hashing is a scrambling or mutation of data using a mathematical function, also known as hashing.

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. So a hash function only works one way.

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

Hash functions are not necessarily secret and accessible and usable by everyone.

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

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

searched and the corresponding input.

9

TRES part21 (not accessible to SBG)

[postal code area(four digits)]TRES

[country of birthPatient (o)]TRES

[homeland Father (o)]TRES

[homeland Mother (o)]TRES

Then the pseudonyms (the hashed values from the PVM, see previous step) in this part

ZorgTTP performed a second pseudonymization run. This uses

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.

This means the following for the pseudonyms received by ZorgTTP:

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

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

pseudonym of the pseudonym.

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

key, then SBG could decrypt the encrypted pseudonym.

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

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

where the.

- 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 (decrypt) to the pseudonym as known in the PVM at the care provider.

- It is not (just) possible for SBG to create a link table. For this cooperation would

are required from ZorgTTP or the healthcare provider.

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

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

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

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

one-way pseudonymization technique, it is possible to use the same pseudonym every time without using a key

to give.”23

After the second pseudonymization pass, the data for ZorgTTP looks like this:

key part

data share

pseudo[pseudoBSN]

21 This data is encrypted by the ZorgTTP offered TRES encryption, whereby SBG does not have access to the data but see aggregated information from it. See reply letter SBG of 25 August 2017, p. 50.

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

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

pseudo[pseudoTorque number]

Encrypted and not transparent for ZorgTTP and is also

not adjusted by ZorgTTP.

pseudo[pseudoCare path number]

pseudo[pseudoDBCTraject number]

TRES part (not accessible to SBG)

[postal code area(four digits)]TRES

[country of birthPatient (o)]TRES

[homeland Father (o)]TRES

[homeland Mother (o)]TRES

The key part and data part are then prepared and retrieved by SBG via the Data Return

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 subsequently encrypted (by ZorgTTP) versions of the citizen service number, link number, care trajectory number and DBCTraject number. The data part consists of the original data (25 data categories) that

are known of a person involved from a mental healthcare provider. In appendix 2 to this report, this is

made clear from a table.

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

outcomes are presented by SBG in the BRaM.24 With BRaM, practice variation can be

treatment outcomes are mapped. Results can be achieved at different levels with BRaM 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 different 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 framework, a gradual phasing out and dismantling of SBG took place in 2018.

There has been an increasingly limited supply of data by healthcare providers and the 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 the connection conditions have been terminated unilaterally and the healthcare providers and health insurers are informed about this December 2018 informed in writing. The last data submissions to SBG took place at the end of November and at the end of December 2018. SBG has stated that it no longer has any data that have been provided to SBG by ZorgTTP. Moreover, SBG no longer has access to data that have formed the basis of the BRaM reports. The database that SBG has in the past built has already been destroyed and so are backup files of the database.26

24 See more detailed reply letter from SBG dated 25 August 2017, p. 24 ff.

25 See SBG reply letter of 16 January 2019 and SBG's opinion 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 - founded on June 1, 2018 - the activities of SBG will be (partially) accommodated and

continued. The infrastructure for supplying data to SBG is hereby transferred to

aka. In addition, the SBG dataset is transferred to Akwa in 'impoverished' 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:

- Birth year, but only for people over 80 years old. Only that group get 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 DBC is 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 if

you are undergoing treatment at institution A and B.

- Postal code area: “The encrypted four digits of the postal code will not be transferred. The derivative

SES and degree of urbanization will be transferred.” The encrypted four digits are TRES encrypted

and were already inaccessible to SBG. SBG already had the SES and urbanization degree. er

thus does not change anything compared to the SBG dataset with regard to this category.

- Patient's country of birth and derived categories (Native, Non-Western immigrant and

western immigrant) thereof. These categories were not required to be submitted and are

optional in MDS.

- Father's country of birth and derived categories (Indigenous, Non-Western immigrant and Western

immigrant) thereof. These categories were not mandatory to provide and are optional in

MDS.

- Mother's country of birth and derived categories (Native, 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

- Respondent type. SBG says about this; “this information 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 supplied.”

- Argus data:29 “the data delivery has barely started, so transferring this data doesn't make sense. Moreover, Akwa GGZ is not commissioned to carry out the Argus registration. Historical 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 is thus inaccessible to SBG and three that are optional could be delivered. This means that of the 25 mandatory data points provided to SBG, 19 data points have been transferred to Akwa. Akwa stands for the following goal with the dataset eyes: enabling historical comparisons in terms of treatment outcomes and to be able to generate patient experiences and associated reports.30 In addition, Akwa will independently to 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 permission for the processing of his/her data. This agreement will be part of the agreement between Akwa and the GGZ providers. The This choice was prompted by the discussions and problems surrounding SBG and the processing of ROM data has occurred and is occurring, not because Akwa believes that the data that they will receive from the mental healthcare providers are personal data.

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

was used for the data collection by SBG. Reference is made to what has been said about this in

paragraph 3.1.31

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

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

4. Review

4.1 Research questions

The key question that must be answered in the present case is whether the data where the

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. In addition, the AP

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

from the Applicant in accordance with 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 so, is there any

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 the request for

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

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

checks against the law that is currently applicable and that is the GDPR. It should be noted, however, that the

terms relevant to this study in the GDPR are virtually unchanged in relation to the Wbp

stayed. The AP is therefore of the opinion that the assessment is materially no different under the GDPR than under the Wbp.

4.2 Does SBG process (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 qualify 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(1) of the GDPR defines as personal data: 'all information about a identified or identifiable natural person ("the data subject"). If becomes identifiable considered a natural person who can be identified, directly or indirectly, in particular by the

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

33 In Article 51 of the General Data Protection Regulation Implementing Act (UAVG) – which entered into force with effect from of 25 May 2018 – it states that the Wbp will be withdrawn.

34 Article 99(2) of the GDPR provides that the GDPR applies from 25 May 2018.

35 By Royal Decree of 16 May 2018 (Staatsblad 2018, 145) the date for establishing 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 is time to be determined by royal decree has been made possible.

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."

The definition makes a distinction, among other things, between direct and indirect traceability. After this, therefore first checked whether the data of SBG can be traced directly to a natural person and subsequently whether indirect traceability is possible.

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 citizen service number, link number, care trajectory number and DBCTraject number. It data part consists of the original data (25 data categories) that are known of a data subject from a mental health care provider. Examples of this data (which are also fully stated in Appendix 2) are gender, year of birth, care provider name, start and end date of the care process.

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

4.2.3 Method of anonymization by SBG and indirect traceability

Now that in the opinion of the AP there is no direct traceability, the question then arises: to or possibly indirect traceability as a result of which a natural person is identified and as a result personal data is involved.

The AP will answer that question on the basis of the provisions of recital 26 of the preamble to the GDPR and recital 26 in the preamble to Directive 95/46/EC. In both considerations, indicated that the data protection principles for any data concerning a identified or identifiable (natural) person. In addition, it has been indicated 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 anonymised to allow indirect traceability to involved is no longer possible. In the opinion of the Data Protection Group Article 29 on anonymization techniques (WP 216 advice 05/2014)36 has examined the question of when such anonymization so that there is no longer any indirect traceability.

Risks in the anonymization process

In the aforementioned opinion of the Data Protection Working Party Article 29 on anonymization techniques (WP 216 advisory report 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

attributen38 would lead to an anonymous dataset. In practice, however, there are still sufficient quasi-identifiers39, other values or attributes with which a person can become identified. The Group mentions a number of steps with which a dataset can be considered anonymous considered, such as “remove attributes and generalize, remove the original data or at the very least” aggregate to a high level of aggregation.”

The above opinion on anonymization techniques states the following about a effective anonymization solution:

“An effective anonymization solution prevents a person from being individualized in a dataset, from two records in a dataset (or in two separate datasets) are related and that from that dataset information is derived. In general, therefore, the removal of directly identifying data is not in itself sufficient to ensure that the data subject is no longer identifiable. Usually need to go further measures are taken to prevent identification. This again depends on the circumstances and the purposes of the processing for which the anonymous data is intended.” (underlined 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 dataset by some or all

highlight records;

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

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

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

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

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

deducibility, being the possibility to measure the value of a personal characteristic ("attribute") with large

probability from the values of a set of other attributes.”

If these risks are sufficiently mitigated or excluded, the used

anonymization solution “sufficiently resistant to re-identification based on the most probable”

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

Mitigation of risks for the SBG . dataset

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

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

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

The following may be noted about the above risks.

Traceability:

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

- Based on the pseudonymised citizen service number, 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

advisory report 5/2014 on anonymization techniques.

39 A quasi-identifier is a combination of attributes related to a data subject or group of data subjects. See for this, 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 opinion advice 5/2014 on anonymization techniques.

- The combination of the other pseudonymised attributes (pair number, care trajectory number, DBC trajectory number) may be unique enough to create a unique record from the to illuminate the data set.
- The combination of the other (not pseudonymised) attributes may also be unique enough to extract a unique record from the dataset.
- The combination of all attributes (both pseudonymized and non-pseudonymized) are unique enough to extract a record from the dataset.

Linkability:

According to SBG, in order to draw up the SBG Benchmark reports, it is necessary to evaluate patients over time and derive information about the success of a treatment in a particular 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 Auxiliary Diagnosis Code) can be derived per record. In addition, the residential area can roughly be derived, because information about the healthcare institution is also known.

It is therefore inherent in this way of benchmarking by SBG that the risks with relating to traceability, linkability and deducibility cannot be removed.

Technical guarantees dataset SBG

In its opinion on anonymization techniques, the Article 29 Working Party writes that

randomizing and generalizing are two ways in which anonymization can be approached.

Randomization includes a group of techniques that “use the truthfulness of data”

modified with the aim of disconnecting that data from the person. If the data is sufficiently random (that is,

say random 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 conversion, but can

offer a solution to the risks of deducibility. Examples of these types of techniques are:

- Noise Addition: Attributes in the dataset are changed in such a way that they are less accurate

to be.

- 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 in which the attributes of

stakeholders are generalized or weakened by changing the scale or scope.

This excludes traceability to the person, but further techniques must be applied

to prevent linkability and deducibility. Examples of generalization techniques:

41 See SBG reply letter of 25 August 2017, appendix 27 about the interpretation 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 merging 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 should be equally distributed

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

with a high degree of uncertainty. T-similarity is a more refined form of this. In the end
these methods must prevent the risk of traceability and deducibility, whereby
it is no longer possible to trace a person with a probabilistic attack or
specific information about a person.

It appears from the documentation received by the AP that no form of
randomization techniques at the time SBG receives the dataset. With regard to generalizing,
the technique of aggregating (not k-anonymity) has been seen, but applied incorrectly. 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. There are in fact 25 quasi-identifiers, which means that within the group of
individualization is still possible in the same year of birth, such as location of care provider, gender,
start date, end date, etc. As a result, the properties of k-
anonymity and L-diversity.

In other words, the SBG dataset is detailed to the extent that on one or more attributes,
pseudonymized or not, a selection can take place in such a way that one individual is removed from the dataset
can become. As a result, insufficient account has been taken of the risks of traceability,
linkability and deducibility and it cannot be about an anonymous dataset.

Pseudonymized data at SBG

The WP 29 opinion on anonymization techniques says the following about pseudonymization:
Pseudonymization replaces one attribute (which is usually unique) in a record with another attribute. The
natural person is therefore still indirectly identifiable. Consequently, pseudonymization in itself is not sufficient to
dataset completely anonymous.

Pseudonymization reduces the linkability between a dataset and the original identity of a data subject, and
is a useful security measure as such, but not an anonymization method.

The pseudonymization method that SBG uses refers to a combination of a hash function and encryption
with a secret key. A hash function has “for an input of any size (a single attribute or
a collection of attributes) output is a fixed size, and cannot be rolled back.” When encrypted with

a secret key “the person holding the key can easily re-identify any data subject by scanning the dataset.”

decode”.

By combining these two methods, the risks of rollback or decryption are reduced,

namely:

- The secret key is known by a trusted third party (ZorgTTP) who does not share it with SBG or

any other party. Decoding by SBG is therefore not possible and SBG cannot therefore dispose of it

about the hashed versions of the citizen service number, link number, DBCTraject number and

Care trajectory number.

18

- The hash function ensures that the trusted third party (ZorgTTP) does not have the original

values of the citizen service number, link number, DBCTraject number and Care trajectory number, but only

about its hashed versions.

- Due to the combination, it is not possible for SBG to build a link table of all BSNs43 with

the corresponding hashed values.

However, the results of this pseudonymization process are per unique BSN, link number,

DBC Track number and Healthcare track number are always the same. In other words, every input yields

always exactly the same output. This ensures that new information can be added over time

to the information already known to SBG.

The aforementioned risks (traceability, linkability and deducibility) are

present pseudonymization process has not been sufficiently removed. For example, traceability to the

person still possible because the person is now identified by a unique value after

pseudonymization. Since the same unique (pseudonymized) values merged over time

should be, the risk of linkability is just as great. Given the amount of data per

pseudonym and the unique combination that this produces makes it possible to identify a person

identify based on this data set. The dataset at SBG is therefore a pseudonymised

data set. The AP considers the position of SBG that it does not receive and/or process 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 is

therefore, with this technical measure, insufficiently removed.

This gives SBG a pseudonymised dataset with personal data that is used

for creating benchmark reports.

Personal data concerning health

In the previous section, the AP established that the data set that SBG receives contains personal data. In

In connection with the prohibition of the processing of personal data relating to health, the following question is:

whether the data that SBG has received are personal data about health.

Article 4(15) of the GDPR defines “health data” as follows:

“data relating to the physical or mental health of a natural person,

including data on health services provided with which information about his

state of health is given

Personal health data includes all data related to the

health status of a data subject and which provide information about the physical or mental

health status of the person concerned in the past, present and future. 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 citizen service number (BSN) is a predictable sequence of numbers.

44 See SBG reply letter 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 establishes that the data set 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. In addition, healthcare providers should also provide a diagnostic code. SBG can place this code next to the code lists owned by 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 data subjects already indicates that the data is related on health. This data, whether in the form of text or attributed 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 (via ZorgTTP) from healthcare providers is personal data contains about health within the meaning of Article 4(15) GDPR.

Processing

The GDPR applies to the processing of personal data. The AP establishes that the reception and storage of the data set by SBG constitutes processing within the meaning of Article 4(2) of the GDPR. SBG has this dataset is retrieved and stored via a digital connection at the Data Return Module (DRM).

This constitutes an automated process that can thus 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 health data within the meaning of Article 4(1) and 15 GDPR.

In addition, the receipt and storage of the data set by SBG is processing within the meaning of Article 4, part 2 GDPR.

Is SBG a controller?

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

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

"a natural or legal person, a public authority, a service 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 that consists 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 SBG reply letter of 25 August 2017, Appendix 3.

SBG has drawn up various conditions and protocols for achieving its goals.

For example, the SBG connection conditions lay down the preconditions to which healthcare providers

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

a data protocol prepared by SBG. In the data protocol, the nature and specifications of the raw data, the

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

minimum required data. While healthcare providers are responsible for the 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 with regard to organizing the activities,

processes and procedures.48

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

quality requirements (standards) SBG must meet. For example, SBG has a quality officer and quality cycle

established, and audits are performed on the quality of information security, privacy,
service provision and realization of SBG information.49 The management of SBG bears ultimate responsibility for the
information security policy that applies to the office environment, employees and
data exchange with organizations and individuals.50

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

Based on the above, the AP concludes that SBG as controller
qualify within the meaning of Article 4(7) GDPR. After all, SBG determines in broad terms and
level of detail which data and how this data arrives at SBG. Healthcare providers who do not
accept connection conditions from SBG cannot purchase services from SBG. In addition, SBG . has
far-reaching responsibilities and decision-making powers over the data set received, such as validity
and its security. This means that SBG can independently make important decisions about the dataset
that she receives from healthcare providers via ZorgTTP and therefore acts as a controller
is designated.

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

The AP has established that the data that SBG has received (via ZorgTTP) from healthcare providers
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 rely on a legal
exception under Article 9 GDPR jo. Article 22 to 30 UAVG.

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

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

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

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

The AP first establishes that SBG cannot invoke one of the general grounds for exception
within the meaning of Article 9 (2) GDPR and Articles 22 and 23 UAVG. To the extent relevant in this study
SBG has not requested explicit permission for the processing from the data subjects, as a result of which
invoking Article 9, second paragraph, sub a GDPR jo. Article 22, second paragraph, sub a of the UAVG does not succeed.
SBG cannot successfully invoke the statutory ground for exception for scientific or
historical research or statistical purposes within the meaning of Article 9, second paragraph, part j of the GDPR jo.
article 24 UAVG. Still undecided whether the processing of health data is necessary
for the purposes of SBG, it is possible to request explicit permission from the
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 statutory grounds for exception with regard to data about
health. SBG does not fall under the aforementioned standard addressees of Article 30 UAVG in which these
statutory grounds for exception have been 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 AVG yo. Article 30(3)(a) of the UAVG, which provides, among other things, that the prohibition on processing
health data does not apply to care providers, institutions or facilities for
healthcare or social services, insofar as the processing is necessary with the
with a view to proper treatment or care of the data subject or the management of the
institution or professional practice.
The AP thus comes to the conclusion that SBG cannot invoke one of the statutory provisions
grounds for exception that could lift the ban on the processing of health data.
As a result, it is prohibited for SBG to use the dataset with
processing personal data about health therein.

4.5 Other grounds for enforcement request

A number of arguments have been put forward by the applicant which have not yet been addressed in this regard
been. The AP sets out 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 whether the way SBG is
furnished and financed justifies the conclusion that SBG cannot become a TTP
qualified, the AP notes that given its role as a supervisory authority on the GDPR and in the past,
under the Wbp in this case must assess whether SBG processes personal data. Now that the AP is of the opinion that
SBG processes personal data about health and does not process this data due to the processing ban
should have been allowed to process, it does not get around to the question of whether or not SBG is a TTP. This also applies
to
doubts raised by the applicant in that regard as to the security of SBG's systems
and the applicable certification.

Key part CareTTP

In its enforcement request, the applicant states that it does not know whether Statistics Netherlands has the option to
key part of ZorgTTP to 'decrypt'. In that regard, she indicates that with 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
indications have been found showing that CBS has the option to
Make sure to 'decrypt' TTP. The encrypted key part and data part are received by the Central
Module TTP (CMT) at ZorgTTP. In this case, only the ZorgTTP CMT has the key to
key to decrypt.

52It concerns Information about diagnoses of patients in hospital care, mental health care and forensic care that

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-providing

5. Akwa . Preview

5.1 Transferred data is personal data

During the investigation it was announced that SBG would cease its activities and a large part of its activities and would transfer the data collected and processed by it to Alliance Quality in the mental health care (Akwa). This was the reason for the AP to also investigate the data transferred by SBG to Akwa. To this end, the AP has asked itself whether the data transferred to Akwa is personal data within the meaning of the GDPR.

As explained in section 3.3.1, SBG transfers a depleted dataset to Akwa. Per record, or so become a data subject of the 25 mandatory attributes (as indicated in the Minimum dataset), 19 transferred to Akwa. These 19 attributes also include the pseudonymised pair number, DBC Track number and Care track number. So these are three of four pseudonymized attributes, but also the primary Diagnostic Code.

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

Given that there are still 19 mandatory categories per record, including the pseudonymised variants of the link number, DBC Trajectory number and Care pathway 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 conversion, linkability and deducibility. The depleted dataset is thus again not anonymized, but still contains pseudonymised personal data relating 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 health data within the meaning of Article 4, parts 1 and 15, of the GDPR, or - before the GDPR came into effect - within the meaning of Article 2, preamble and under a, of the Wbp. This is because the data that SBG received was insufficiently anonymized, so that it the risk of indirect traceability was insufficiently removed. Furthermore, the AP concludes that SBG could not invoke one of the statutory grounds for exception for this processing that it ban on processing health data. This results in the SBG was prohibited on the basis of Article 9(1) of the GDPR to use the dataset containing personal data processing about health.

7. View SBG

SBG made its view on the report known to the AP on 27 June 2019. SBG partly responds to the legal assessments of the report and partly on the factual inaccuracies and omissions. Below the AP first responds to the factual inaccuracies and omissions alleged by SBG. The addition to the facts has not led to a different legal valuation. The AP further notes that in the In the context of the objection procedure, a full reconsideration takes place, including the grounds/opinion from SBG.

7.1 Opinion on factual inaccuracies and omissions

View SBG

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

SBG, for example, there is no distinction between the four different data processing activities of SBG whole.

Response AP

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

View SBG

Section 3.1.1 states that SBG was set up by stakeholders under the supervision of VWS, under more GGZ Nederland and Zorgverzekeraars Nederland. This is correct in itself, but according to SBG is missing that at the time also the National Platform GGz (LPGGz), the umbrella organization of 20 patient and family organizations and now MIND, was involved in the creation of SBG.

Response AP

The AP does not consider the addition of SBG relevant to the report. Like SBG in the 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 for the present legal assessment.

View SBG

Section 3.1.1 of the report states that BRaM reports to the National Health Care Institute were provided. In the opinion of SBG, this is incorrect, the National Health Care Institute did not receive a BRaM reports delivered. BRaM reports were generated for goal 2a and 2b only.

Response AP

The AP has removed the National Health Care Institute from the relevant sentence.

View SBG

In section 3.1.2 of the report, the figure includes Vektis as a party to which SBG provides data would have delivered. However, according to SBG, there has never been any data delivery by SBG to Vektis occurred. This was the intention, as can be read in the Data protocol for secondary objective 2f but has never been realized. That is why this data flow was included in the data flow sketch of June 26, 2017, which is enclosed as Appendix 18 to the reply letter dated August 25, 2017.

Response AP

The AP has removed Vektis from the image, as it does not determine the present legal case rating.

View SBG

It was noted in paragraph 3.1.2 in footnote 19 of the report that for predictable and common inputs, calculate the output. In the opinion of SBG, this is technically incorrect, a hash can never be computed in reverse no matter how frequent (common) an input is. There is no traceable pattern that can lead to predictability.

Response 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 regard, the AP notes the following.

The AP agrees that in "normal" cases (i.e. 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 ascending numbers) or common (for example, a simple password) then a table with input and its hash (de output) are calculated. Should one have a hash, which is known to be a predictable input (for example, one number from an increasing series of numbers) then one can trivially use all hashes of hash the integer sequence again one by one. Then the hash can be looked up in the just calculated list and thus the original input has become known. With this process, the hash function repeated to arrive at the same output and then find out the input (to Search).

View SBG

It is stated in paragraph 3.2 of the report that SBG only employs one employee who

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.

Response 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 SBG

The research questions are set out in section 4.1 of the report. The research questions are according to SBG worded carelessly, incomplete and out of order.

Response AP

The AP does not follow this view. The AP considers the research questions to be correct and in the correct order stated. 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 basis is applicable must only be established if there is a processing of

personal data by a controller and after the ban on the processing of special personal data can be withdrawn.

View 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.

Response AP

The AP does not follow this view. The AP has in various sections, such as from section 4.2.2 to with 4.4, states on which articles of law, considerations and guidelines it has based its findings based. SBG is of course free to argue what this lacks.

View SBG

In a general sense, it is not possible to speak of sound and sufficiently substantiated conclusions, certainly not with regard to SBG's qualification as a controller and with regard to the fact that SBG cannot invoke a legal exception to the prohibition of processing personal data concerning health. Both conclusions are drawn on the basis of only some paragraphs. In addition, in a general sense, a careful assessment of the SBG arguments put forward and of the substantiation of SBG's views.

Response AP

As mentioned above, the AP will in the next phase, in which the parties also agree on a express an opinion session on the findings of the AP, consider the alleged legal positions and qualifications.

7.2 Summary of SBG zienswijze view

General

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

View of SBG controller

According to SBG, no (clear) distinction is made in the research report between the four various data processing activities by SBG.54 While these all have a separate and careful require legal qualification, which is completely absent from the report.

First of all, SBG states that it is not a controller for the four data processors activities now that SBG has no specific legal capacity, no implied authority, nor does it

54 The four data processing activities are:

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

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

2b. Benchmarking with (anonymous) ROM information extra setting, allowing institutions to compare or compare themselves be able to make regional comparisons

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

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

28

has the actual influence to determine the purpose 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 of the healthcare provider. SBG thus notes that it is therefore (a delegation of) patients from the GGZ, healthcare providers and healthcare insurers was/were jointly and in fact in broad outlines and in level of detail determined which data and in what way data came in to SBG, in which this moreover was partly prompted by requirements that followed from the legal obligations to supply data to Zorginstituut Nederland and Argus data. The application of connection conditions can nor lead to the qualification of SBG as a controller.

The far-reaching responsibilities and decision-making powers regarding the received dataset, with regard to of validity and security thereof, were also not independently exercised by SBG. It always became actions of SBG, its management and employees, in fact framed by the patients' comments on this agreements made by the GGZ, care providers and health insurers. From independent and/or decisive influence of (the management of) SBG on determining the goals of the data processing activities and the resources were thus out of the question. If and to the extent that SBG's influence with regard to the deploying resources under the data processing activities for purpose 2 was greater than appropriate in the role of pure processor, there was at most a question of joint 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 qualify as a processing agreement.

Response AP

The controller is the person who, alone or jointly with others, determines the purpose and means of
for the processing of personal data.55 SBG processes, as explained above in this report
set, personal data; it receives personal data and sets requirements for how it should be processed
delivered 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. SBG then qualifies
also not as a processor, but as a controller. That in the processing chain, in addition to SBG
other (joint56) controller or exercise influence on SBG, without prejudice
that SBG is a data controller. Under the responsibility of its board, SBG is, as it turns out
follows from the Data protocol of SBG, charged with the analysis of the personal data they receive via TTP
receives information as well as for developing, managing and making available SBG information and
related applications to the users.
In light of and in addition to the foregoing, the AP notes the following. SBG is
responsible for compiling comparison information for health insurers,
patient organizations and healthcare providers. To this end, SBG indicates in detail which information it provides
the individual healthcare providers must be provided via ZorgTTP in order to be able to measure and
benchmark. On the basis of SBG's Conditions of Connection57, the healthcare provider must pay all

55 Article 4(7) of the GDPR.

56In this regard, 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 affect the individual responsibility of one of the
(joint) responsible persons. cf. CJEU, C□131/12 (Google Spain SL and Google Inc./Agencia Española de Protección de Datos
(AEP)), 13 May 2014, par. 40. Each of the controllers is responsible for all data processing and compliance
of the associated 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 for
healthcare providers”. The
Conditions of connection contain the conditions that a healthcare provider must meet in order to be able to use the services of
SBG

to provide relevant so-called 'Raw Data' to ZorgTTP. In the Minimal 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 trajectory, the secondary diagnosis, the practitioner, the DBC trajectory58, the measurements and the items. To give a good and true picture of the treatment outcomes, the healthcare provider is also obliged to provide information about the number of DBCs within its organization. The SBG Data protocol also contains instructions to the healthcare provider what information should be submitted and how. The board of SBG may decide to adopt the Data protocol change in accordance with the provisions of the articles of association.

The Data Protocol also states which data is provided to third parties, under what conditions and for what purposes. In that context, the Data Protocol provides for a review by the board of SBG, in collaboration with the SBG Scientific Council. It is therefore SBG that determines where the its analyzed (aggregated) data.

From the foregoing, the AP concludes that SBG does indeed have the purpose and means of processing personal data and thus 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 regard, the AP finds that SBG for the benefit of the various data processing activities receives one set of data on which the Conditions of Connection and the SBG's data protocol apply and the personal data is processed by SBG accordingly incorporated.

View 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 involved in the processing activities of SBG. SBG has set out the principles on which the healthcare provider can appeal, 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 may perform on the basis of the legal basis of the healthcare provider. The healthcare provider can, according to

SBG for the measuring instruments task invoke Article 6, first paragraph, sub c GDPR. For the intra-setting
For benchmarking with ROM, the healthcare provider can invoke Article 6, paragraph 1, sub b and c of the GDPR.
In addition, the healthcare provider can benchmark with ROM for the extra institution on the basis of Article 6,
first paragraph, sub c GDPR and potentially also at sub b. With regard to offering the digital safe,
for the purpose of scientific research, the healthcare provider may invoke Article 6, paragraph 1, sub b
GDPR. Finally, for keeping the Argus registration, the healthcare provider can, according to SBG
invoke Article 6(1)(c) of the GDPR.
Furthermore, SBG argues that it is not they, but the healthcare provider who is relying on a legal exception to the ban
processing of personal data relating to health. Assuming
personal data is involved, according to SBG, the healthcare provider can undertake the measuring instruments task
invoke Article 9, second paragraph, sub i GDPR. For the intra-setting benchmarking with ROM, the
healthcare provider invoke Article 9, second paragraph, sub h AVG in conjunction with Article 30, third paragraph, preamble
and
under sub a UAVG. As for the additional setting benchmarking with ROM, it is possible that the
healthcare provider cannot invoke the statutory exception of Article 9, second paragraph, sub h in conjunction with
to make. In addition, the Conditions of Connection describe the role of SBG as a data broker and contain the preconditions of
the instruction to be given to ZorgTTP by the GGZ provider.
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 resources
where that determination relates to 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, preamble and under a UAVG. For the storage of information provided by the healthcare provider to
SBG
data supplied for scientific research in the digital safe may be the basis

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

Response AP

The AP does not follow SBG's view and notes the following about this. Because SBG in the judgment of the AP qualifies as a controller and not as a processor, it independently serves a fruitful appeal to one of the exceptional grounds for the entrusted to it personal data about health (a special categories of personal data) process. 60 The AP explained with reasons that SBG cannot do that.

View SBG permission and anonymization

According to SBG, the AP seems to suggest that asking for explicit permission from the patient is the only possibility to collect 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 one theory assumes that either (explicit) consent is required, or that data is anonymous must be. Now that the AP de facto sets the bar for anonymous so high that this is practically unfeasible, you come automatically with (explicit) permission. According to SBG, this means that there is a black or white approach, without recognizing the shades of gray in between. Moreover, it fails to recognize that asking (explicit) consent in the context of data processing for serious quality registrations disadvantages, as well as that complete anonymization leads to incorrect results. SBG asks the AP for to reconsider this position critically.

Response AP

The AP is of the opinion, as detailed in the report, 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 is unable to do this, 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 results, is - whatever else of that - a as a result of applicable laws and regulations as well as choices made in connection with the

setting up and setting up of SBG. However, the AP sees no reason in this regard to make a different statement 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 the WP29 opinion quoted by the AP does not serve as a benchmark for determining whether the data is sufficient be anonymized. In the opinion of SBG there are two other and related criteria that should be taken as the starting point when answering the question whether data is sufficient are anonymized.

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 danger of identification in reality seems insignificant. 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.

Second, according to SBG, the 'motivated intruder test' described by the Information . is relevant Commissioner's Office (ICO), the UK privacy regulator, in the document “Anonymisation: managing data protection risk. Code of Practice”. The relevant question is whether it is for a motivated intruder, in view of his knowledge and available resources such as time, money and manpower, reasonably it is possible to identify natural persons in the anonymized data that SBG receives from Stichting ZorgTTP to identify. According to SBG, the answer to the above question is in the negative. Moreover it is about the possibility to identify and not about the possibility to individualize. SBG lights this as follows.

SBG is unable to extract the encrypted and encoded attributes from the data provided by ZorgTTP on behalf of the healthcare provider to decrypt Source XML file provided to SBG. Now that SBG cannot be deemed able to decrypt the encrypted and encoded attributes from the Source XML file that

ZorgTTP, it is also unlikely that a motivated intruder could commit this decryption
reasonably be able to. A motivated intruder will refuse the cooperation of ZorgTTP and the
healthcare provider to decrypt and identify, which cooperation of course
will be remembered. If the motivated intruder already had access to the sufficient
anonymized dataset, he is dependent on the use of illegal means, such as hacking or
break into the systems of ZorgTTP and/or the healthcare provider in order to decrypt. The
however, the necessity to deploy such illegal means means that there is no longer any question of
reasonable means of identification. 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 has a sufficient
is an anonymized file, so that SBG does not receive any personal data.
According to the AP, it is possible for SBG to use the same pseudonym (from the
pseudonym), individualize a person in a dataset. In the opinion of SBG, this is correct.
According to SBG, the question then arises whether when the possibility of individualization (and thus
not to identify!) exists, this leads to indirect traceability and thus to the
qualification personal data. According to SBG, the answer to that question is in the negative, while the AP
assumes an affirmative answer.
The AP then points to three risks mentioned in the opinion that must be taken into account when
anonymization process, i.e. the chance of traceability, linkability and deducibility. the AP
concludes, after discussing the three risks, that SBG does not sufficiently mitigate them. With reference to
De Tekst & Commentaar 'Privacy and telecommunications law' states that SBG should 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 anonymized data
identify. By using the wrong criterion to determine whether indirect
traceable data, the AP was not able to come to the (interim) conclusion that SBG personal data
processed.
In addition, SBG also appoints the Minister of Health, Welfare and Sport (“VWS”) in

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

on the basis of which 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 application of pseudonymization in accordance with five conditions leads to sufficient anonymized data. SBG notes in this context that it seems that the AP has previously implicitly (!) has let go of the advocated approach. It may of course be the case that new insights which result in an old approach no longer being 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 according to the audit reports submitted, SBG was allowed to use it confidence to meet the conditions that were part of the old approach. This delivers according to SBG is contrary to the principle of legal certainty.

Response 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 Court's ruling on Breyer goes in the opinion of the AP not on. This case concerns only the indirect traceability of dynamic IP addresses. In addition,

no additional information available from the online media service provider. As a result, it should
necessarily turn to the Internet Service Provider to resolve the dynamic IP address
to a person. In SBG, however, there is much more to any pseudonymised patient
information available. It is not just one data point, as is the case with the dynamic IP address,
but dozens.61 In view of the type of data and the number of data processed on one patient
over a longer period of time, there is therefore (the risk of) indirect conversion to more parties and public
sources cannot be avoided. The AP also notes that the choice of SBG to treat patients
individualizable in combination with the choice to use directly identifying personal data
pseudonymization leads to a potentially vulnerable system that carries a real risk of identification
brings. In this regard, the AP notes that through a request for access to personal data, a
data subject to the healthcare provider and subsequently to SBG can legitimately be traced
to make.
Where SBG refers to the 'motivated intruder test', the AP notes the following. With regard to a
motivated intruder with data from different 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, through the combination of this data and taking into account the
current available technology and the constant and rapid development that the technology is going through
very plausible. In addition, the AP emphasizes that SBG, as a controller,
should also explicitly take future situations and developments into account. They referred
to the 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 has no information that can be traced back to the
person
gets delivered. In this regard, the AP notes that as an independent supervisor, in view of the
its assigned task, independently and independently assesses whether there is
personal data and this is separate from the minister's opinion on this and explains in

for example answers to parliamentary questions.

61 For more information, 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
the question whether the processing of personal data comes to a different conclusion than the
the authors of the audit reports, the AP notes that it has explained in this report with reasons
why it is of the opinion that there is (a processing of) personal data. The AP sees against that
background 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 sufficiently anonymised
data, it is stated in the letter from the Dutch DPA that the processed data is not indirectly identifying
may be. As explained above, in the case of SBG's data, this is now
not really a question. The AP therefore does not see that the conditions mentioned in the letter from the Dutch DPA are
released.

34

Attachment 1

Course of the investigation

By letter dated 24 March 2017, the applicant requested the AP to take enforcement action against SBG.
The AP subsequently informed SBG of the enforcement request.
By letter dated 24 April 2017, SBG responded to the enforcement request.
In a letter dated 1 May 2017, the applicant was asked for further substantiation of the request.
On May 23, 2017, the AP received the requested substantiation.
In a letter dated May 30, 2017, the AP informed SBG that it was opening an investigation into the processing
of personal data by SBG. In that letter, the AP asked SBG questions.
The AP also informed the applicant in a letter dated 30 May about the start of this investigation.
On 2 August 2017, a judgment in summary proceedings was rendered in respect of the present issue, with

SBG as defendant.62 The preliminary relief judge ruled that it is not sufficiently plausible

It has become apparent that personal data are being processed within the meaning of the Directive 63 and the Wbp.

By letter dated 25 August 2017, SBG answered the questions of the AP.

On September 11, 2017, the applicant was informed by e-mail that the AP is still working on the

assessment of the information received from SBG and the significance of the judgment in preliminary relief proceedings.

By letter of 5 February 2018, the applicant expressed its concerns in writing to the AP regarding the

supply of medical data by GGZ institutions to SBG, because the applicant had

learned that a third of mental health care institutions had continued with this. In this the applicant saw

reason to request the AP to immediately suspend the delivery of data to SBG pending the investigation

to have it laid.

By e-mails dated 22 and 31 January 2018, 17 February 2018 and 30 March 2018, the applicant submitted additional

information sent to the AP.

By letter of 18 April 2018, the applicant gave notice of default to the AP due to the lack of a decision

on its enforcement request. On 2 May 2018, the applicant withdrew the notice of default.

On 11 July 2018, the AP had a conversation with SBG in which it was explained by SBG that it will shortly

only wants to process data 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 email 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 20 November 2018, the AP received a written notice of default from the applicant.

The AP was further informed by letter on 27 November 2018 by SBG about the

future/discontinuation of SBG.

On December 3, 2018, the AP decided on the enforcement request. The enforcement request is hereby 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 again on January 9, 2019 by regular and registered mail as well as by e-mail on January 8, 2019 to applicant, when it appeared that the registered mail item had not been collected.

On 14 December 2018, SBG and Akwa were requested to provide further information.

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

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

The AP has granted the applicant a period to supplement its grounds ending on February 13 2019.

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

By e-mail of February 6, March 14 and April 30, 2019, SBG, in response to her on 16 January 2019 provided additional information if requested.

Appendix 2

1. Data Processing PVM

The table below64 contains three columns. The first column describes the data before processing by the PVM, second column after processing by the PVM and the third column has what kind of processing occurred. The '(o)' indicates that this information can be provided optionally. With red is indicate which data is processed into pseudonyms in the PVM and is marked in blue which data is aggregated and encrypted with TRES. The red part is made by ZorgTTP key part and the other data 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

is transparent for ZorgTTP. The substantive data part (displayed in black) will only become transparent again

at SBG during the later steps.

Data for editing by PVM66

Data after processing by PVM

Type of processing that has

Without Argus data

Healthcare provider:

Healthcare provider name

Healthcare provider code

Patient:

Social Security Number

occurred

Pseudo Social Security Number

A BSN is hashed to pseudoBSN.

The original citizen service number (BSN) will be deleted and

not delivered.

Educational attainment

Age situation

homelandMother (o)

[homeland Mother (o)]TRES

The country is encrypted with TRES and not

For SBG this is converted to

accessible to SBG. It will be

origin categories: autochthonous,

stored by SBG.

non-western immigrant and western

immigrant.

homelandFather (o)

[homeland Father (o)]TRES

This is TRES encrypted and not

For SBG this is converted to

accessible to SBG. It will be

origin categories: autochthonous,

stored by SBG.

64 Compiled from the documents:

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

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

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

- Factsheet_pseudonymization_CareTTP_2017

- Appendix 27 - MDS explanation per variable

65 See Factsheet_pseudonymization_CareTTP_2017

66 This is based on the MDS, the XML file examples (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 to

accessible to SBG. It will be

origin categories: autochthonous,

stored by SBG.

non-western immigrant and western

immigrant.

Postal code area

[postal code area(four digits)]TRES

“These are still being prepared by ZorgTTP before

[these are the four digits of the zip code]

Four digits of the zip code are

reception at SBG TRES-encrypted and

TRES encrypted and are not

aggregated to two major

insightful for SBG, see step 4b.

case mix variables namely

Urbanization degree (5 groups) and Social

For SBG, the zip code is converted

Economic Status (5 groups). SBG

by SES value and degree of urbanization.

does not receive a zip code.”

Pseudo Pairing Number

A pairing number is hashed to

pseudomatch number. The original

is removed and not delivered.

Pseudo care trajectory number

A care trajectory number is hashed

to pseudo care trajectory number. It

original is deleted and not

delivered.

Sex

Year of birth

Pairing number

Care trajectory

end dateCare trajectory

start dateCare trajectory

GAFscore

primaryDiagnosisCode

Location code (o)

care domainCode

care trajectory number

Secondary diagnosis code

secondary diagnosisCode

practitioner

Occupation (0)

Alias (0)

primaryorcousins (0)

DBCTraject67

reasonEndDBC

67 Multiple DBC trajectories per patient can be specified

dateLastSession

dateFirstSession

end dateDBC

start dateDBC

DBCPperformanceCode

ReasonNonResponsePre-measurement

ReasonNonResponseNameting

DBC Track number

Pseudo DBC Track number

A DBCTraject number is hashed

to pseudo DBCTraject number. It

original is deleted and not

delivered.

Measurement68

total scoreMeasurement

usedMeasuring instrument

typeRespondent

earthMeasurement

Type measurement

Date

Item69

Rating (0)

item number(0)

Argus data is added to

above data

Argus_Recording

end dateRecording

start dateRecording

argus_episode

Location code

legalFramework

DegreeResistance

TypeMeasure

enddatetimeEpisode

startdatetimeEpisode

Argus_LegalStatus

LegalStatusCode

end dateLegalStatus

68 Multiple measurements can be made per DBC trajectory

69 Multiple items can be specified per measurement.

start dateLegalStatus

2. Data SBG as available in the DRM

The table below shows the data as available in the DRM at SBG, before it was 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

[homeland Mother (o)]TRES

This is TRES encrypted and not accessible by SBG.

It is saved by SBG.

The origin category (native, non-western immigrant

and western immigrants) is known to SBG.

[homeland Father (o)]TRES

This is TRES encrypted and not accessible by SBG.

The origin category (native, non-western immigrant

It is saved by SBG.

and western immigrants) is known to SBG.

[country of birthPatient (o)]TRES

This is TRES encrypted and not accessible by SBG.

The origin category (native, non-western immigrant

It is saved by SBG.

and western immigrants) is known to SBG.

[postal code area(four digits)]TRES

This was the postcode area at the care provider, whose

SES value

Urbanization degree

Sex

Year of birth

pseudo[pseudoTorque number]

Care trajectory

end dateCare trajectory

start dateCare trajectory

GAFscore

primaryDiagnosisCode

Location code (o)

care domainCode

pseudo[pseudoCare path number]

Secondary diagnosis code

secondary diagnosisCode

practitioner

Occupation (0)

Alias (0)

four digits are encrypted with TRES.

It is saved by SBG.

40

primaryorcousins (0)

DBCTraject70

reasonEndDBC

dateLastSession

dateFirstSession

end dateDBC

start dateDBC

DBCPperformanceCode

ReasonNonResponsePre-measurement

ReasonNonResponseNameting

pseudo[pseudoDBCTraject number]

Measurement71

total scoreMeasurement

usedMeasuring instrument

typeRespondent

earthMeasurement

Type measurement

Date

Item72

Rating (0)

item number(0)

Argus data will be added to above

data

Argus_Recording

end dateRecording

start dateRecording

argus_episode

Location code

legalFramework

MateResistance

TypeMeasure

enddatetimeEpisode

startdatetimeEpisode

70 Multiple DBC trajectories per patient can be specified

71 Multiple measurements can be made per DBC trajectory

72 Multiple items can be specified per measurement.