Findings VGZ

1. Code of Conduct and Privacy Policy

VGZ stated in its letter of 25 October 2017 that the cooperative VGZ UA consists of five insurance entities: VGZ Zorgverzekeraar N.V. (VGZ, NV Univé Zorg (Univé), IZA Zorgverzekeraar NV (IZA), IZZ Zorgverzekeraar NV (IZZ) meanwhile changed to VGZ voor de Zorg N.V., and NV Health insurer UMC (UMC). In 2017, VGZ Cares N.V. also merged with VGZ Zorgverzekeraar N.V. VGZ applies the same policy for all these legal entities.

VGZ reports that it processes personal data of (prospective) insured persons, policyholders, employees who fall under a company care scheme through their employer and clients who fall under the Long-term Care Act (Wlz) that are served through the VGZ Care Office.

VGZ states as processing purposes:

- Entering into and executing the insurance contract (regular personal data and personal data concerning health);
- Implementing the Wlz (regular personal data and personal data regarding the health);

Provision of information (regular personal data);

- Marketing purposes (regular personal data);
-
- Investigations (regular personal data and personal data concerning health);
- Ensuring the security and integrity of our sector (regular personal data and criminal data);
- Complying with legal obligations.

VGZ indicates that it uses the following documents when processing personal data:

a) the Health Insurers' Code of Conduct for the Processing of Personal Data by Zorgverzekeraars Nederland;

b) the Uniform Measures drawn up by ZN, in particular the Uniform Measures relating to to Functional unit (01), Privacy Statement (02), Providing information to insured persons and

policyholder (03), Direct Marketing (04), Privacy statement handling (06),

Information exchange health insurers in auditing and fraud control (08), Use

means of authentication for internet applications (09);

c) the Protocol Material Control version 31 October 2016 of ZN;

d) the GGZ Privacy Regulation as laid down in Article 3.5 of the Specialized Regulations

mental health care from the Dutch Healthcare Authority (NZa) (currently NR/REG-1734);

e) the Protocol Incident Alert System Financial Institutions.

VGZ also uses the following documents in addition to or for further elaboration of the

Code of Conduct

f) the Privacy Text and its Privacy Statement on its website;

g) [CONFIDENTIAL]

h) [CONFIDENTIAL]

i) [CONFIDENTIAL]

j) [CONFIDENTIAL]

k) CISPO job description;

l) [CONFIDENTIAL]

m) [CONFIDENTIAL]

n) [CONFIDENTIAL]

o) Standard 04 – Logical Access Security;

p) [CONFIDENTIAL]

q) Standard 07 – Business Operations Security;

r) [CONFIDENTIAL]

s) [CONFIDENTIAL]

t) [CONFIDENTIAL]

u) [CONFIDENTIAL]

v) [CONFIDENTIAL]

w) [CONFIDENTIAL]

x) [CONFIDENTIAL]

y) [CONFIDENTIAL]

z) [CONFIDENTIAL]

aa) [CONFIDENTIAL]

bb) [CONFIDENTIAL]

With regard to the formal and material audit, VGZ indicates that it has policy documents in

supplement to the Code of Conduct for Healthcare Insurers. For example, an internal code of conduct has been drawn up, as

well as a

overview of frequently asked questions. [CONFIDENTIAL]

VGZ states that it is transparent about the way in which it carries out the checks and provides information about this

published on its website:

https://www.vgz.nl/privacy

https://www.vgz.nl/privacy/wetten-en-regelen

https://www.vgz.nl/nieuws/medische-data-inzien-mag-vgz-dat

[CONFIDENTIAL]

[CONFIDENTIAL] Does it follow from the report that there is a deviation from the code of conduct or

Uniform Measure then a risk assessment takes place in which the privacy impact is investigated.

[CONFIDENTIAL] also ensured that any changes in legislation and regulations by the department

Legal Affairs are being implemented. [CONFIDENTIAL]

[CONFIDENTIAL]

Rating

In addition to the Code of Conduct for Healthcare Insurers and the Uniform Measures of Healthcare Insurers in the

Netherlands

(ZN) VGZ uses various policy documents, work processes and work instructions. These are on the

AP submitted.

The AP also notes that the privacy policy and the way in which personal data are processed
be periodically checked by means of [CONFIDENTIAL] From the submitted documents it is further
ensure that VGZ takes into account changes in legislation and regulations and relevant case law.
The AP also concludes from the documents that VGZ pays attention to awareness with regard to the
applicable privacy legislation. [CONFIDENTIAL]
In view of the foregoing, the mere circumstance that VGZ states on its website that it

application of the code of conduct, which has since been rejected, does not already indicate that VGZ is acting in violation of
the Wbp.
2. Digital declaration without diagnostic information
VGZ points out that declarations containing personal data, including personal data
relating to health, are processed by VGZ employees who work at the
[CONFIDENTIAL]. This concerns employees with [CONFIDENTIAL] who have this
process personal data for the purpose of payment of declared assets. Hereby
activities are carried out in accordance with Uniform Measure 03 Providing information to insured persons
and policyholder. In addition, from their position, employees of the [CONFIDENTIAL]
authorized to have access to personal data relating to health in order to
Health Insurance Act (Zvw).
With regard to the privacy regulation, VGZ has put forward the following. From the research of the NZa
from 2016 into the way in which health insurers apply the privacy regulation, it follows that the regulation
is carried out correctly by VGZ, as VGZ points out. VGZ has indicated that it will participate in this
makes use of the Uniform Measure for privacy settlement of declarations (06) of ZN.
VGZ also indicates that after the NZa's investigation in 2016 into the implementation of the privacy regulation
has not made any adjustments with regard to the implementation of this scheme because it
investigation showed that VGZ adequately implemented the privacy regulation. Insofar as the NZa recommendations
regarding controls, VGZ chose [CONFIDENTIAL] on its own initiative. VGZ

has submitted the [CONFIDENTIAL] and the NZa report with findings for explanation. also has

VGZ followed the recommendations of the NZa by devoting continued attention to following

[CONFIDENTIAL]. VGZ has added to this by drawing up a periodic assessment

take in the [CONFIDENTIAL]. This also includes the recommendation to deviate from the

the advice of the medical adviser. In addition, VGZ has followed the NZa's recommendation that

medical advisors who are involved in purchasing from a particular healthcare provider are not also involved

during checks at that healthcare provider and to record this in the check-up process.

Rating

For the way in which VGZ handles privacy statements and requesting information from the

insured persons, the AP refers to the NZa study from 20161, which was conducted in consultation with the AP

executed. In that study, the NZa concluded that the degree of compliance with the privacy regulation

of the NZa is generally good.

The AP endorses the findings as recorded in that investigation. During the present investigation

The AP has not revealed any changes in the policy or working method of VGZ that would require further consultation

research on this point.

3. Target binding

-marketing

1 https://www.nza.nl/1048076/1048181/Report_Zorgverzekeraars_controles_en_privacyreglement_september_2016.pdf

VGZ indicates that it does not process personal health data for

marketing purposes. For this purpose, it only uses regular personal data. about this

is communicated transparently in the privacy statement on the VGZ website. Insured persons can

always invoke the right to object. Insured persons who have invoked this will be

excluded from any marketing campaign.

VGZ has submitted an example of a number of documents showing its working method with regard to

a marketing plan shows: [CONFIDENTIAL] result of a sample campaign.

VGZ has explained that the marketing process consists of the following steps: [CONFIDENTIAL].

-exception to target limitation

Insofar as the Health Insurers Code of Conduct allows for an exception to the purpose limitation principle, VGZ indicates that in exceptional cases it makes use of the possibility laid down in Article 3.13 of the Code of Conduct.

In its letter of 12 December 2017 to the AP, VGZ explained that it uses the exception of article 3.13 of the Code of Conduct for reporting, for example, fraud or requisition of data by the police, the judiciary and the tax authorities in the event of fraud. also has

VGZ has indicated that it makes use of the Uniform Measure 08 - Exchange of personal data between health insurers in various forms of control and fraud control - in addition to the Code of Conduct. VGZ explains that it is recorded in the data subject's file that personal data are shared, with whom, what the purpose of this is and what the considerations have been. [CONFIDENTIAL]. The guidelines of ZN and the Dutch Association of Insurers are also used, such as 'handling information at the Loket Insurance Fraud'. [CONFIDENTIAL]

The AP has had access to the work instructions to which VGZ refers.

Rating

The AP notes that there is no question of setting aside the purpose limitation requirement for arbitrary purposes. For example, it has not been shown that the processing of personal data relating to the health for marketing purposes. On the basis of the documents submitted, VGZ made it plausible that both the marketing communications and the internal assessment process that preceding, are not based on personal health data.

When asked, VGZ has indicated that it, like the other health insurers, makes use of the exception as referred to in Article 3.13 of the Code of Conduct or Article 43 of the Wbp in the event of a declaration of or requests for information on cases of fraud where information must be provided to the police, the judiciary and/or the tax authorities. The basic principle of VGZ is that, in principle, also in those cases no personal data concerning health are provided. This only happens if it is explicitly

be claimed, for example in the cases where Articles 126nf and 126uf of the Code of
Provision of criminal proceedings. These benefits are handled by the [CONFIDENTIAL] and may
only take place with the consent of a medical advisor. These benefits and the
consent of the medical advisor are recorded in writing in the file of the person concerned.
More specifically, it is established on the basis of which legal basis, to whom and which

personal data, including personal data relating to health, is provided, why
this is necessary and what weighting has taken place in this regard.
For the provision of personal data (relating to health) to the police, the judiciary, the
The tax authorities and statutory supervisors have a basis, namely a statutory
obligation, as referred to in Article 8, opening words and under c, of the Wbp. These benefits are in
in accordance with Article 43, opening words and under b, c, and d, of the Wbp. In the case of such
provision is made in accordance with the Uniform Measure 8 of ZN, in addition to Article 3.13 of
the Code of Conduct for health insurers, as well as the guideline ‘handling tools for reporting insurance fraud at the Loket’ and
internal work instructions. These documents contain a sufficiently specific elaboration of this article
for health insurers. This means that VGZ makes use of supplementary policy in which Article 3.13 of
the Code of Conduct has been elaborated for the benefit of health insurers and there is a lawful
exception.
The underlying information does not show any unlawful provision by VGZ to
third parties, now that there is a legal basis and in principle only regular personal data
are provided and no personal data concerning health. Are personal data
concerning health, this will only take place after the medical adviser has determined whether there is any
is a basis for this provision and the provision of this data is necessary. The AP has
furthermore, do not receive any indications or signals that offer leads for another
conclusion. It has therefore not been shown that VGZ provides more personal data for this purpose than
necessary and it has not been shown that VGZ provides personal data without

basis would exist.

4. Unauthorized access to personal data

[CONFIDENTIAL]

The following is important with regard to VGZ's security policy. [CONFIDENTIAL]

The following is important with regard to the systems with which VGZ works. VGZ uses different systems and applications for their business processes. VGZ has an application overview supplied with a description of various applications in which personal data is incorporated. [CONFIDENTIAL]

The following is important with regard to the authorization policy. [CONFIDENTIAL]

During the on-site investigation, VGZ stated that [CONFIDENTIAL] is a so-called certification round is held, during which the responsible manager accepts all the granted authorizations checks and approves.

[CONFIDENTIAL]

With regard to logging, VGZ has put forward the following. [CONFIDENTIAL]

Rating

- authorization policy

[CONFIDENTIAL] However, the AP recommends VGZ to develop the authorization policy in this way work that as a main rule it is established per function (group) which roles and authorizations for necessary for the performance of that function.

-logging

In the answers of 25 October 2017, VGZ states: [CONFIDENTIAL]

-conclusion

VGZ has organized its corporate culture in such a way that only employees are allowed access have access to personal data relating to health insofar as this is necessary for the purpose for which the employees process the personal data. For example, VGZ has established that:

marketing employees are not allowed to process personal data relating to health.

However, the investigation by the AP shows that a number of employees of the Customer and

VGZ brand partners actually have access to personal health data, while

this is not necessary for their work. Being able to consult personal data is

pursuant to Article 1, preamble and under b, of the Wbp, to be regarded as processing personal data.

VGZ therefore does not have adequate technical resources to ensure that employees do not

have had access to personal data that is not necessary for the purpose for which they

are processed. [CONFIDENTIAL]

The foregoing leads to the conclusion that VGZ does not have appropriate technological measures such as

referred to in Article 13 of the Wbp.

The AP has in the submitted documents that show how a marketing campaign is carried out at VGZ

carried out, incidentally, no indications were found for the conclusion that marketing employees

actually process personal health data for a marketing campaign. That does

however, does not detract from the conclusion that Article 13 of the Wbp has been violated, because the technological

measures taken by VGZ are not appropriate.

5. Editors

VGZ has indicated that it uses [CONFIDENTIAL] external information for [CONFIDENTIAL]

processors for the processing of personal data relating to health. It's about

various organisations, ranging from call centers and collection companies, to ICT organizations and

organizations engaged in expense scanning and printing, graphic finishing,

inserting and sending other printed matter. A list of editors has been submitted.

In its letter, VGZ states that safeguarding legislation and regulations regarding personal data is

generality means that [CONFIDENTIAL] is involved in the project start, whereby the purchasing process

is being run through. [CONFIDENTIAL] that there is (possibly) processing of personal data,

then [CONFIDENTIAL] takes care of drawing up the processor agreement. A fully completed

processing agreement is delivered to the [CONFIDENTIAL] who adds it to the

main agreement.

[CONFIDENTIAL] checked whether a processor agreement is still up to date. [CONFIDENTIAL] wears

adjust the policy, specific instructions or implement additional/amended

policy, etc.

VGZ has sent along its standard processor agreement. This includes the obligations for the

editors and any sub-editors are explicitly elaborated. This includes compliance with the

Wbp, the requirements of strict purpose limitation, confidentiality, security and control, data breach notification obligation, the

engaging a sub-processor only with written permission from VGZ and timely

destruction of personal data.

Rating

The AP has taken note of the aforementioned documents and standard texts and contracts.

In this, VGZ has further elaborated on the Code of Conduct for Healthcare Insurers. Furthermore, this shows

that processors must also comply with the special requirements that apply from the Wbp with regard to the

processing of personal data concerning health. For example, editors are obliged to

take technological and organizational measures to protect personal data

concerning health and also to comply with the Wbp, including the reporting obligation

data leaks from Article 34a of the Wbp. It follows from the standard agreement and standard text that VGZ

supervises correct compliance with the Wbp. Processors are thus explicitly pointed out to the special requirements

that apply from the Wbp with regard to the processing of personal data relating to health and

the secrecy. [CONFIDENTIAL] The AP concludes from this that the obligations that

are laid down in Article 14 of the Wbp in conjunction with Articles 12, 13 and 34a of the Wbp.

6. Medical professional secrecy

VGZ has set up various functional units (FEs). Employees working within an FE

fall under the functional responsibility of the medical advisor. At VGZ are [CONFIDENTIAL]

employs medical advisers, all of whom are registered in accordance with the BIG Act. [CONFIDENTIAL] The

medical advisor who heads an FE is responsible for complying with the

privacy rules and the other internal preconditions for handling medical data. The

medical advisor has a functional responsibility for complying with the internal

rules of conduct by an FE. The medical advisor monitors that the FE functions as intended and that the

The privacy awareness of the employees and managers is at a sufficient level. [CONFIDENTIAL]

[CONFIDENTIAL]

With regard to the confidentiality agreements, VGZ has put forward the following. Processing

personal data about a person's health takes place within VGZ under functional management

from a medical advisor. [CONFIDENTIAL]

Rating

-confidentiality

In the first place, the AP notes that the medical advisors who direct the FEs are and are all doctors

registered in accordance with the BIG Act (BIG-registered). They are therefore subject to a duty of confidentiality

rest by virtue of profession.2

All employees of VGZ are subject to a duty of confidentiality under a

(non disclosure agreement. [CONFIDENTIAL] Based on the submitted documents, the

AP that organizational measures have been taken to ensure that employees who

actually process personal data concerning someone's health

sign non-disclosure agreements and that there is sufficient control.

In view of this, the AP comes to the conclusion that VGZ complies with the provisions of Article 21, first paragraph, preamble

and under b of the Wbp, read in conjunction with the second paragraph, now the personal data concerning the

health are processed by persons who, by virtue of their profession or by virtue of a

agreement are subject to a duty of confidentiality.

-necessity requirement

VGZ has fleshed out the role of the medical advisor by assigning tasks to so-called

FEs processing personal health data under responsibility

from a medical advisor. When designing the FEs, VGZ took into account the Uniform

Measures regarding the Functional Unit of ZN and the Framework Functional Unit Controls. the AP

establishes on the basis of the documents that the medical advisor has a clear role in the context of the

handling health data within his/her business unit. [CONFIDENTIAL]

In view of the foregoing, the AP concludes that VGZ, with its chosen interpretation of the

role of the medical adviser has sufficiently ensured that the assessment or interpretation of the

necessity for the processing of personal data relating to health in accordance with the

Wbp and the Zvw is carried out by someone with sufficient (medical) knowledge.

-detail check

The question whether health insurers act in accordance with Article 7.8 of the Rzv is part of the

based on the study that the NZa conducted in 2016 – in consultation with the AP. The NZa has

concluded on the basis of that investigation that none of the health insurers committed a violation on this point

to commit. During the current investigation, the AP did not find any leads at VGZ to:

to doubt the findings of the NZa on this point.

-conclusion

In view of the foregoing, the AP concludes that with regard to medical professional secrecy, VGZ

does not act in violation of the Wbp.

2 Pursuant to Article 88 of the BIG Act, anyone who practices a profession in the field of individual healthcare is,

is obliged to observe secrecy that has been entrusted to him in the exercise of his profession. In addition, a medical

duty of confidentiality, as laid down in Section 7:457 of the Dutch Civil Code (BW), also referred to as the

medical treatment agreement.

Conclusions

Below is a conclusion for each part.

Code of Conduct and Privacy Policy

In view of the use of the Uniform Measures and VGZ's own privacy policy, the AP of

believes that the mere fact that VGZ states on its website that it applies the code of conduct,

which has since been rejected, not already that VGZ is acting in violation of the Wbp.

Digital declaration without diagnostic information

The AP endorses the findings as recorded in the cited study by the NZa. During the day

the current investigation by the AP has not revealed any changes in policy or working methods

of VGZ that should lead to a further investigation on this point.

Target binding

The AP has not shown any unlawful provision by VGZ to third parties, now that there is a

legal basis and in principle only regular personal data are provided and no

personal data concerning health. Are personal data relating to health

provided, this will only take place after the medical advisor has determined whether there is a basis for this

provision and provision of this data is necessary. Moreover, the AP has no

receive clues or signals that offer leads for a different conclusion. Therefore,

it has not been shown that VGZ provides more personal data for this purpose than is necessary and

Nor has it been shown that VGZ provides personal data without there being any basis for doing so.

Unauthorized access to personal data

VGZ has organized its corporate culture in such a way that only employees are allowed access

have access to personal data relating to health insofar as this is necessary for the purpose

for which the employees process the personal data. For example, VGZ has established that:

marketing employees are not allowed to process personal data relating to health.

However, the investigation by the AP shows that a number of employees of the Customer and

VGZ brand partners actually have access to personal health data, while

this is not necessary for their work. Being able to consult personal data is

pursuant to Article 1, preamble and under b, of the Wbp, to be regarded as processing personal data.

VGZ therefore does not have adequate technical resources to ensure that employees do not

have had access to personal data that is not necessary for the purpose for which they
are processed. [CONFIDENTIAL]
The foregoing leads to the conclusion that VGZ does not have appropriate technological measures such as
referred to in Article 13 of the Wbp.
The AP has in the submitted documents that show how a marketing campaign is carried out at VGZ
carried out, incidentally, no indications were found for the conclusion that marketing employees
actually process personal health data for a marketing campaign. That does
however, does not detract from the conclusion that Article 13 of the Wbp has been violated, because the technological
measures taken by VGZ are not appropriate.
Editors

It follows from the standard agreement and standard text that VGZ supervises correct compliance with the
Wbp on this point. Processors are thus explicitly pointed out to the special requirements that apply from the Wbp at least
with regard to the processing of personal data relating to health and confidentiality.
[CONFIDENTIAL] The AP concludes from this that the obligations laid down in
Article 14 of the Wbp in conjunction with Articles 12, 13 and 34a of the Wbp.
Doctor-patient confidentiality
The AP comes to the conclusion that VGZ does not act in conflict with regard to medical professional secrecy
with the Wbp.
The AP concludes that personal data concerning health are processed within VGZ
processed by persons who are subject to a duty of confidentiality by virtue of a profession (physician) as well as
from an agreement (VGZ employees). In view of this, the AP comes to the conclusion that VGZ complies with
the provisions of Article 21, first paragraph, opening words and under b, of the Wbp, read in conjunction with the
second member.
Furthermore, the AP comes to the conclusion that VGZ, with its chosen interpretation of the role of the medical
advisor has sufficiently ensured that the assessment or interpretation of the need for the

processing of personal data regarding health in accordance with the Wbp and the Zvw
is carried out by someone with sufficient (medical) knowledge.
The question whether health insurers ultimately act in accordance with Article 7.8 of the Rzv
Finally, part of the study that the NZa conducted in 2016 – in consultation with the AP
conducted. On the basis of that study, the NZa concluded that none of the health insurers
point committed a violation. During the current investigation at VGZ, the AP did not have any
leads were found to doubt the findings of the NZa on this point.