VGZ findings

1. Code of Conduct and Privacy Policy

VGZ indicated 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). VGZ Cares N.V. also merged with VGZ Zorgverzekeraar N.V. in 2017. VGZ applies the same policy to all these legal entities.

VGZ informs that it processes personal data of (prospective) insured persons, policyholders, employees who fall under an occupational health 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);
- Execution of the Wlz (regular personal data and personal data concerning 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 Code of Conduct for the Processing of Personal Data Healthcare Insurers of Zorgverzekeraars Nederland;

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

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

Exchange of information between health insurers during checks and fraud control (08), Use

means of authentication for internet applications (09);

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

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

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

e) the Protocol Incident Warning 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) Job description CISPO;

l) [CONFIDENTIAL]

m) [CONFIDENTIAL]

n) [CONFIDENTIAL]

o) Standard 04 – Logical Access Protection;

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 inspection, VGZ indicates that it has policy documents in place

addition to the Health Insurers Code of Conduct. For example, an internal code of conduct has been drawn up, as well as a

overview of frequently asked questions. [CONFIDENTIAL]

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

published on its website:

https://www.vgz.nl/privacy

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

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

[CONFIDENTIAL]

[CONFIDENTIAL] It follows 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 laws and regulations by the department

Legal Affairs are being implemented. [CONFIDENTIAL]

[CONFIDENTIAL]

Judgement

In addition to the Health Insurers Code of Conduct and the Uniform Measures of Health Insurers in the Netherlands

(ZN) VGZ uses various of its own 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 checked periodically by means of [CONFIDENTIAL] From the documents submitted, further details can be found

ensure that VGZ takes account of changes in legislation and regulations and relevant jurisprudence.

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 means that it

application of the code of conduct, which has meanwhile been rejected, does not mean that VGZ is acting contrary to the Wbp.

2. Digital declaration without diagnosis information

VGZ argues that invoices containing personal data, including personal data regarding health, are processed by employees of VGZ who work at the [CONFIDENTIAL]. This concerns employees with [CONFIDENTIAL] who have this process personal data for the purpose of payment of claimed credits. Hereby work is done in accordance with Uniform Measure 03 Providing information to insured persons and policyholder. In addition, employees of the [CONFIDENTIAL] authorized to have access to personal data concerning 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 to the way in which health insurers apply the privacy regulation, it follows that regulation is carried out correctly by VGZ, VGZ puts forward. VGZ has indicated that it will participate in this uses the Uniform Measure privacy handling declarations (06) of ZN.

VGZ also indicates that after the NZa's investigation into the implementation of the privacy regulation in 2016, it has not made any adjustments with regard to the implementation of this scheme because the investigation showed that VGZ adequately implemented the privacy regulation. As far as the NZa recommendations has done regarding checks, VGZ has opted for it on its own initiative [CONFIDENTIAL]. VGZ has submitted the [CONFIDENTIAL] and the NZa report with findings by way of explanation. Also has VGZ followed the recommendations of the NZa by continuing to pay attention to monitoring

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

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

advice from the medical advisor. VGZ has also followed the recommendation of the NZa that

medical advisers who are involved in the procurement of a particular healthcare provider are not also involved

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

Judgement

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

policyholders, the AP refers to the NZa study from 20161 that is 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 study. During the present investigation

the AP has not further revealed any changes in VGZ's policy or working method that lead to a further

research on this point.

3. Purpose Limitation

marketing

1 https://www.nza.nl/1048076/1048181/Rapport_Zorgverzekeraars_checks_en_privacy regulations_september_2016.pdf

VGZ indicates that it does not process personal data concerning health 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 can

always invoke the right of opposition. Insured persons who have invoked this will be

excluded from a 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].

purpose limitation exception

Insofar as the Code of Conduct for Health Insurers allows for an exception to the
purpose limitation principle, VGZ indicates that in exceptional cases it makes use of the
option laid down in Article 3.13 of the Code of Conduct.
VGZ explained in its letter of 12 December 2017 to the AP that it uses the
with the exception of Article 3.13 of the Code of Conduct for reporting fraud, for example
requisition of data by the police, the judiciary and the Tax and Customs Administration in the event of fraud. Also has
VGZ hereby indicates that it uses 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 personal data is recorded in the file of the person concerned
are shared, with whom, what the purpose is and what the considerations have been.
[CONFIDENTIAL]. The guidelines of ZN and the Dutch Association of Insurers are also used,
such as 'Handles for reporting the Insurance Fraud Office'. [CONFIDENTIAL]
The AP has had access to the work instructions referred to by VGZ.
Judgement
The AP has established that the purpose limitation requirement has not been set aside
arbitrary purposes. For example, there has been no evidence of the processing of personal data concerning the
health for marketing purposes. Based on the documents submitted, VGZ
made plausible that both the marketing communications and the internal assessment process are related to this
foregoing, are not based on personal health data.
When asked, VGZ stated that, just like the other health insurers, it uses the
exception as referred to in Article 3.13 of the Code of Conduct or Article 43 of the Wbp when reporting or
information requests regarding fraud cases where information must be provided to the police,
judiciary and/or the tax authorities. VGZ's starting point is that, in principle, no
personal data concerning health are provided. This only happens if it is explicit
be claimed, for example in cases where articles 126nf and 126uf of the Code of
Provide for criminal prosecution. These provisions are handled by the [CONFIDENTIAL] and may

only take place with the consent of a medical adviser. These provisions and the
consent of the medical adviser are recorded in writing in the file of the person concerned.
This is more specifically laid down on the basis of which legal basis, to whom and which

personal data, including health data, are provided, why
this is necessary and what weighting has taken place.
For the provision of personal data (concerning health) to the police, the judiciary, the
There is a basis for the Tax and Customs Administration and statutory supervisors, namely a statutory one
obligation, as referred to in Article 8, preamble and under c, of the Wbp. These transfers are in
in accordance with article 43, preamble and under b, c, and d, of the Wbp. In case of such
provision is made of the Uniform Measure 8 of ZN, in addition to Article 3.13 of
the Health Insurers Code of Conduct, as well as the guideline 'Guidelines for declaration Loket Verzekeringsfraude' and
internal work instructions. These documents contain a sufficiently specific elaboration of this article
for health insurers. This means that VGZ uses supplementary policy in which Article 3.13 of
the Code of Conduct has been elaborated for the benefit of health insurers and is lawful
exception.
The underlying information does not reveal any unlawful provisions 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. become personal data
regarding health, this will only take place after the medical adviser has determined whether there is
is a basis for this provision and the provision of this data is necessary. The AP has
moreover, no instructions or signals are received that provide leads for another
conclusion. It has therefore not become apparent that VGZ provides more personal data for this purpose than
is necessary and it has also not been shown that VGZ provides personal data without a
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 processed incorporated. [CONFIDENTIAL]

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

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

[CONFIDENTIAL]

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

Judgement

authorization policy

[CONFIDENTIAL] However, the DPA recommends that VGZ formulate the authorization policy as follows work that as a general rule applies that per function (group) it is determined which roles and authorizations for necessary for the exercise of that function.

-logging

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

-conclusion

VGZ has organized its corporate culture in such a way that only employees are allowed access to personal data concerning health insofar as this is necessary for the purpose for which the employees process the personal data. For example, this has been laid down by VGZ marketing employees are not allowed to process personal data concerning health.

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

Brand partners of VGZ actually have access to personal data concerning health, while
this is not necessary for their work. Being able to consult personal data is
to be regarded as the processing of personal data pursuant to Article 1, preamble and under b, of the Wbp.
VGZ therefore does not have sufficient 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 suitable technological measures at its disposal
referred to in Article 13 of the Wbp.
In the documents submitted, the AP has indicated how a marketing campaign at VGZ is carried out
Incidentally, no indications were found for the conclusion that marketing employees
actually process personal data concerning health for a marketing campaign. That does
however, does not alter the conclusion that Article 13 of the Wbp has been violated, because the technological
measures taken by VGZ are not appropriate.
5. Processors
VGZ has indicated that it uses [CONFIDENTIAL] external under [CONFIDENTIAL].
processors for the processing of personal data concerning health. It's about
various organizations, ranging from call centers and debt collection companies, to ICT organizations and
organizations involved in expense scanning and printing, graphic finishing,
inserting and sending other printed matter. A list of processors has been submitted.
In its letter, VGZ indicates that safeguarding legislation and regulations regarding personal data is in its favour
generality means that [CONFIDENTIAL] is involved in the project start, including the procurement process
is run through. [CONFIDENTIAL] that there is (possible) processing of personal data,
then [CONFIDENTIAL] will take care of drawing up the processor agreement. A fully completed
processor agreement is delivered to the [CONFIDENTIAL] who adds it to the

master agreement.

[CONFIDENTIAL] checked whether a processor agreement is still current. [CONFIDENTIAL] carries
make sure to adjust the policy, specific instructions or implementation of additional/changed
policy etc.
VGZ has included its standard processor agreement. This includes the obligations for the
processors and any sub-processors 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 in good time
destruction of personal data.
Judgement
The AP has taken note of the aforementioned documents and standard texts and contracts.
VGZ has further elaborated 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, processors are obliged to
take technological and organizational measures to protect personal data
with regard to 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
monitors proper compliance with the Wbp. Processors are thus explicitly informed of the special requirements
that apply from the Wbp with regard to the processing of personal data concerning 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 confidentiality
VGZ has set up various functional units (FEs). Employees who work within an FE
fall under the functional responsibility of the medical advisor. At VGZ [CONFIDENTIAL]
employed medical advisers, all of whom are registered in accordance with the BIG Act. [CONFIDENTIAL] The
medical advisor in charge of 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 compliance with the internal

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

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

[CONFIDENTIAL]

With regard to the non-disclosure agreements, VGZ has put forward the following. Processing

personal data about someone's health takes place within VGZ under functional control

from a medical advisor. [CONFIDENTIAL]

Judgement

-confidentiality

The AP first of all notes that the medical advisors who manage the FEs are and are all doctors

registered in accordance with the BIG Act (BIG registered). This means that they have a duty of confidentiality

rest on account of profession.2

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

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

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

actually process personal data concerning someone's health

sign confidentiality agreements and that there is sufficient guidance on this.

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 paragraph, now the personal data concerning the

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

agreement are subject to a duty of confidentiality.

-necessity requirement

VGZ has fulfilled the role of the medical adviser by assigning tasks to so-called

FEs in which personal data related to health are processed under responsibility

from a medical advisor. VGZ has taken the Uniform into account when designing the FEs
Measures regarding the Functional Unit of ZN and the Framework of Functional Unit Controls. The AP
establishes on the basis of the documents that the medical adviser has a clear role in the context of the
handling of health data within his/her business unit. [CONFIDENTIAL]
In view of the foregoing, the AP comes to the conclusion that VGZ's 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 concerning health in accordance with the
Wbp and the Zvw is carried out by someone with sufficient (medical) knowledge of the matter.
- detail check
The question of whether health insurers act in accordance with Article 7.8 of the Rzv is part of this
based on the research that the NZa conducted in 2016 – in consultation with the AP. The NZa has run out
Based on that investigation, it was concluded that none of the health insurers committed a violation on this point
to commit. During the present investigation at VGZ, the AP did not find any leads to
to doubt the findings of the NZa on this point.
-conclusion
In view of the foregoing, the AP comes to the conclusion that VGZ with regard to medical confidentiality
does not act in violation of the Wbp.
2 Pursuant to Section 88 of the BIG Act, anyone who practices a profession in the field of individual health care is
obliged to observe secrecy with regard to matters entrusted to him in the exercise of his profession. In addition, a medical one
also applies
duty of confidentiality, as laid down in Section 7:457 of the Dutch Civil Code (BW), also referred to as the Law on
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 is of

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

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

Digital declaration without diagnosis information

The AP endorses the findings as recorded in the NZa study referred to above. During the day

the AP's current investigation has not revealed any further changes in policy or working methods

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

Purpose limitation

The AP has not found 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. Become personal data concerning health

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

provision and provision of this data is necessary. The AP also has none

receive indications or signals that provide leads for a different conclusion. Therefore

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

nor has it become apparent that VGZ provides personal data without a 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

to personal data concerning health insofar as this is necessary for the purpose

for which the employees process the personal data. For example, this has been laid down by VGZ

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

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

Brand partners of VGZ actually have access to personal data concerning health, while

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

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

VGZ therefore does not have sufficient 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 suitable technological measures at its disposal referred to in Article 13 of the Wbp.

In the documents submitted, the AP has indicated how a marketing campaign at VGZ is carried out
Incidentally, no indications were found for the conclusion that marketing employees
actually process personal data concerning health for a marketing campaign. That does
however, does not alter the conclusion that Article 13 of the Wbp has been violated, because the technological measures taken by VGZ are not appropriate.

Processors

It follows from the standard agreement and standard text that VGZ supervises correct compliance with the Wbp on this point. Processors are thus explicitly referred to the special requirements that apply from the Wbp ten with regard to the processing of personal data concerning 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 violation of medical professional secrecy
with the Wbp.

The AP concludes that personal data concerning health within VGZ
processed by persons subject to a duty of confidentiality by virtue of a profession (doctor) as well
from an agreement (VGZ employees). In view of this, the AP concludes that VGZ complies
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 adviser has sufficiently ensured that the assessment or interpretation of the need for the

processing of personal data concerning health in accordance with the Wbp and the Zvw

is carried out by someone with sufficient (medical) knowledge of the matter.

Finally, the question of whether health insurers act in accordance with Article 7.8 of the Rzv is an issue

Finally, part of the investigation that the NZa conducted in 2016 – in consultation with the AP

conducted. On the basis of that investigation, the NZa has concluded that none of the health insurers on this

commit a violation. During the present investigation at VGZ, the AP did not have any

leads to doubt the findings of the NZa on this point.