Menzis findings

1. Code of Conduct and Privacy Policy

The following risk bearers belong to the Menzis Group: Menzis Zorgverzekeraar N.V., Menzis N.V. and Anderzorg N.V. This also includes implementation of the Long-Term Care Act (Wlz) by Stichting Zorgkantoor Menzis, insofar as it concerns insured persons of Menzis. The information provided by Menzis applies for all named legal entities.

Menzis indicates that it processes personal data of insured persons on the basis of the Health Insurance Act (Zvw), the Long-Term Care Act and with regard to persons who have (additional) health insurance have closed. Processing takes place for the purposes of: execution of the insurance contract, for commercial purposes (legitimate interest) and due to legal obligations. As far as personal data concerning health are processed, this is done within the framework of the implementation of the insurance, Menzis puts forward.

Menzis also processes personal data of healthcare providers, employees, potential customers and persons who have registered for the SamenGezond program.

Menzis 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.

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

Code of Conduct:

f) Menzis policy for the protection of personal data;

g) data retention and destruction directive;

h) provide directive data to third parties;

i) guideline Privacy organization;

j) Inspection and correction procedure;

k) Right of opposition procedure;

l) Data processing notification procedure;

m) Misdirected Medical Records Procedure;

n) Model agreement for the delivery of personal data;

o) compliance with the Code of Conduct for the Processing of Personal Data by Health Insurers;

p) Scientific statistical research;

q) Protocol on the obligation to report data breaches;

r) Information Security Policy;

s) Regulations for setting up a Functional Unit;

t) Non-disclosure agreements (text of employment contract, functional units, etc.).

u) Explanation activities Compliance Function;

v) Thematic framework compliance 2017 version E&Y;

w) Presenter update privacy policy, guidelines and procedures;

x) Logical access security policy guideline;

y) Menzis segregation of duties policy 3.0;

z) Consent statement SamenGezond;

aa) Working document contract guide;

bb) SCB Privacy and Security Measures;

cc) Article 15 AIV Privacy and Information Security.

Menzis has explained that it has a compliance control framework, which it uses to assess whether

the correct implementation of privacy laws and policies. This system consists of a
detailed excel overview with a list of all parts to be tested from various so-called
surveillance areas. For example, the provisions of current and future privacy laws and regulations are stated
and the standard to be tested, which criteria must be met in order to be able to conclude that
the standard has been met and how proof must be provided. The business units
van Menzis are periodically fully assessed on the application of the control measures from the
compliance control framework. One of the purposes of this is to adapt Menzis' privacy policy to
applicable laws and regulations and other relevant developments, including jurisprudence.
The Data Protection Officer and the [CONFIDENTIAL] operate a risk-based
and thematic approach to control the safeguarding of privacy. The entire organization becomes every
[CONFIDENTIAL] with regard to the selected risks and themes. All clusters (total
[CONFIDENTIAL]) within Menzis that have to do with the processing of personal data
involved. This leads to a report with a score of whether these components are met. It
latest research dates from [CONFIDENTIAL] and has led to follow-up on various points of attention
[CONFIDENTIAL] conducted.
With a view to the arrival of the General Data Protection Regulation (GDPR) as of May 25, 2018
Menzis has drawn up a new control framework in collaboration with [CONFIDENTIAL], based on
whose organization will be assessed for compliance in the fourth quarter of 2017. Ahead
on the GDPR, Privacy Impact Assessments are already being carried out for the most important business functions,
including the corporate functions [CONFIDENTIAL]
The starting point of Menzis is that the use of personal data concerning health is exclusive
permitted for employees who need this information due to their position and activities and
if the necessity test (proportionality and subsidiarity requirements) is met. This
starting point is embedded in the culture of Menzis through its privacy policy, awareness
programs and the training program for new employees (e-learning) and the continuous
training program for existing employees. All employees are required to have one

sign a confidentiality agreement and comply with it. Leaders emphasize this
repetition. Awareness for compliance with applicable laws and regulations that pertain to the protection of
personal data is encouraged as much as possible. Since [CONFIDENTIAL] there are around this
themed annual activities, such as a 'Week for privacy', in which all employees are aware

be made aware of what is and what is not allowed in this area. Further policy changes
discussed. Last year, this week consisted, among other things, of reenacting concrete incidents
actors, followed by an explanation of the permitted course of action. This week also consisted of giving
of information, and questions could be asked about privacy. Menzis has continued to use
mystery guests tested whether there is (possible) non-compliance with the standards in practice. This is
further tested using a fake phishing email. Also the introduction of the obligation to report data breaches
and the advent of the GDPR play a relevant role in this context. Managers are responsible for that
their employees are kept informed about important developments, as well as responding to them
specific files are reviewed.

Judgement

The Dutch Data Protection Authority (AP) concludes that Menzis does not exclusively use the
Code of Conduct, but also applies the Uniform Measures of Health Insurers in the Netherlands (ZN),
as well as various own policy documents, work processes and work instructions. The AP has knowledge
taken from all submitted documents. These documents are further elaborated in concrete
work processes and work instructions that are focused on the activities of Menzis as
health insurer. The AP further notes that Menzis has provided processes for the
monitoring compliance with its privacy policy.

The AP also notes that Menzis ensures that the privacy policy is adjusted to changes in
laws and regulations and jurisprudence.

Finally, the AP concludes from the interviews and supplied documents that Menzis pays attention
to proper compliance with applicable laws and regulations that pertain to the protection of

personal data. The employees become

of Menzis as much as possible aware of the way in which personal data should be handled

handled. The AP concludes from these activities that Menzis attaches importance to correct compliance with the

applicable laws and regulations as well as its privacy policy as laid down in supplementary

documents, work processes and work instructions.

In view of the foregoing, the mere circumstance that Menzis states on its website means that it

application of the code of conduct – which has meanwhile been rejected, does not mean that Menzis is acting in violation

with the Personal Data Protection Act (Wbp).

2. Digital declaration without diagnosis information

In response to a ruling by the CBB that health insurers must provide for a privacy regulation

on the basis of which mental health care patients must be able to declare information without stating a diagnosis,1

the NZa provided a regulation in March 2012. Following on from this, Menzis has in her

insurance conditions since 2014 include the following text as standard:

! NB

If you do not want the diagnosis code to be stated on the declaration, but still submit the declaration for reimbursement

eligibility, a statement is required prior to or at the latest with the first invoice. You serve with

have your practitioner sign a statement and send it to Menzis. This statement can be found at

1 CBB 2 August 2010, ECLI:NL:CBB:2010:BN3056.

www.menzis.nl/toeslagen.

Menzis has also explained that, in response to the NZa's investigation in 2016, it was through

of entering form letters ensures that in case an insured makes use of

a privacy statement, you will no longer be asked for the integral referral letter or treatment plan.

Judgement

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

policyholders, the AP refers to the NZa study from 20162, which 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

from the AP there has been no further evidence of changes in Menzis' policy or working methods that lead to a further

research on this point.

3. Purpose Limitation

marketing

Menzis indicates that it does not process any personal data concerning health for

marketing purposes. An exception to this is the health program “SamenGezond”. In the

As part of this program, personal data relating to health will only be processed with

express consent of the participant. If the participant withdraws his consent, then

the program is terminated.

Menzis has explained how a regular marketing campaign is established internally. [CONFIDENTIAL]

After a draft action has been approved within the [CONFIDENTIAL], it will then be submitted

to, among others, the [CONFIDENTIAL]. These departments assess, among other things, whether for implementation

of the marketing campaign personal data is processed, or no use is made of it

personal data concerning health, as well as whether the (regular) personal data that are

processed are necessary for the intended purpose. This follows from the documents submitted

marketing employees only select recipients of any marketing action on the basis

of regular personal data such as name, address, e-mail and telephone details, designation man or

woman and date of birth or insurance product. This was confirmed during the interviews. An example of

a marketing campaign has been submitted in the form of a newsletter. The example gives no clues

that its recipient has been selected on the basis of personal health data.

purpose limitation exception

Insofar as the Code of Conduct allows for an exception to the purpose limitation principle

Menzis indicates that it does not actively use this option as laid down in article

3.13 of the Code of Conduct.

Menzis has stated that it will only in the event of a declaration or if it has a

claim from the police or judicial authorities, or the Tax and Customs Administration, applies Article 3.13 of

the Code of Conduct and proceeds to provide personal data (concerning health). At the

2 https://www.nza.nl/1048076/1048181/Rapport_Zorgverzekeraars_controles_en_privacy regulations_september_2016.pdf.

provision of personal data is made use of the Uniform Measure 8 of ZN. A

provision as at issue here is always recorded in writing and concerns a decision taken on

management level is taken after a positive advice from the [CONFIDENTIAL]. A list of

claims from the police, judiciary or tax authorities for 2017 have been submitted by Menzis to the AP.

[CONFIDENTIAL]

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

Menzis made plausible that both the marketing communications and the internal assessment process

preceding it, are not based on personal data concerning health.

The AP notes that Menzis makes use of the option that is available in exceptional cases

included in Article 3.13 of the Code of Conduct. This provision is almost identical to Article 43 of the

Wbp.

Only in the event of a declaration by Menzis or claims by the police, the judiciary and the Tax and Customs Administration

Menzis provides personal data. This mainly concerns cases of fraud. The premise of

Menzis is that, in principle, no personal data concerning health will be processed in those cases either

provided. This only happens if they are explicitly demanded (for example, in the cases where the

Articles 126nf and 126uf of the Code of Criminal Procedure). These supplies are

only possible with the (written) consent of the management and are recorded in writing

For the provision of personal data (concerning health) to the police, the judiciary, the
The Tax and Customs Administration (and statutory supervisors) have a basis, 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, as well as internal
policy documents, in addition to Article 3.13 of the Code of Conduct. The Uniform measure 8 contains to
the opinion of the AP a sufficiently specific elaboration of this article for health insurers. From the
underlying information has not revealed any unlawful provision by Menzis
third parties now that there is a legal basis and in principle only regular personal data
are provided and no personal data concerning health. Therefore, it has not been shown
Menzis provides more personal data for this purpose than is necessary and has also not been shown
that Menzis provides personal data without a legal basis for doing so. The AP
moreover, has not received any instructions or signals that provide leads for another
conclusion.

4. Unauthorized Access to Personal Data

[CONFIDENTIAL]

Judgement

authorization policy in general

[CONFIDENTIAL]

- authorizations of employees of the marketing department

[CONFIDENTIAL]

In addition to this, the following is important. Although Menzis has made it clear that
employees are constantly made aware of the way in which they handle personal data concerning the
health and that this is monitored by their superiors through
of the weekly file checks, it is not possible for Menzis to check whether her

employees adhere to it in practice. [CONFIDENTIAL]

The AP has not yet established that marketing employees actually use personal data

processing health data for the purpose of carrying out marketing campaigns. [CONFIDENTIAL]

-conclusion

Menzis has organized its corporate culture in such a way that only employees have access

may have access to personal data concerning health insofar as this is necessary for the

purpose for which the employees process the personal data. For example, by Menzis

stipulates that marketing employees are not allowed to share health-related personal data

process.

However, the investigation by the AP shows that marketing employees of Menzis do in fact have access

to personal data concerning health. 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.

Menzis therefore does not have sufficient technical resources to guarantee this

employees do not have access to personal data that is not necessary for the purpose

for which they are processed. In that context, the AP points out that Menzis, for example, does not have any log files

keeps track of access to personal data, including special personal data.

The foregoing leads to the conclusion that Menzis does not have suitable technological measures

as referred to in Article 13 of the Wbp. The AP has underlying documents that show how

a marketing campaign at Menzis is carried out, however, no indications were found for the

conclusion that marketing employees actually collect personal data concerning health

processing for a marketing campaign. However, this does not alter the conclusion that Article 13 of the Wbp is

violated, because the technological measures that Menzis has taken are not appropriate.

5. Processors

Menzis has indicated that it has agreements with a total of [CONFIDENTIAL] processors

and uses standard texts and contracts for this in which the provisions of the Wbp and the

Code of Conduct have been further developed. The standard texts and contracts used by Menzis are on

submitted to the AP. These have already been adjusted by Menzis in light of the AVG.

Judgement

The AP has both the standard texts and contracts and a completed version of a
processing agreement received. The AP concludes from this that those agreements provide for a

translation of the obligations arising from the Wbp and the Code of Conduct for the processors of Menzis and that this is a further elaboration of the provisions of the Health Insurers Code of Conduct. be like that processors are, among other things, obliged to take technological and organizational measures to security of personal data with regard to health and also to comply with the Wbp, including the obligation to report data leaks from Article 34a of the Wbp. From the standard agreement and standard text follows that Menzis supervises correct compliance with the Wbp. Editors become like this explicit reference to the special requirements that apply on the basis of the Wbp with regard to the processing of personal data concerning health. Based on this, the AP concludes that Menzis on this point, the obligations laid down in Article 14 of the Wbp in connection with Articles 12, 13 and 34a of the Wbp.

6. Medical confidentiality

Menzis indicates that it works with [CONFIDENTIAL]. Each FE is controlled by a medical counselor. [CONFIDENTIAL]

Menzis has explained the following with regard to confidentiality.

FE employees are required to sign a non-disclosure agreement upon joining. The The confidentiality statement is part of Menzis' individual employment contracts employees and these employees are also based on the applicable collective labor agreement (CAO) kept confidential. Employees who work in an FE sign in connection with it processing of personal data concerning health, in addition, an additional FE-non-disclosure agreement. Menzis employees who have customer contact must also take an oath or make a promise to keep secret what they have been entrusted with on the phone. In

In addition to these measures, privacy awareness programs are conducted annually through
of e-learning, presentations in work meetings by the Data Protection Officer and/or
the Compliance officer, visits by a mystery guest and video messages from the CEO.
Menzis has explained the following about the role of the medical adviser.
The medical adviser broadly determines whether and which personal data concerning health
are necessary and, for example, must be requested from a healthcare provider. As much as possible
we work with standard instructions and work processes in which the protection of personal data
are embedded. These instructions and work processes have been drawn up in part by the medical adviser and are being
updated
at least [CONFIDENTIAL] reviewed and adjusted. This will happen sooner if necessary.
Menzis further explained during the interview that if requested, it will also
from performing a detailed check at file level at a healthcare provider on site to the work
of a medical advisor.
The (team) manager(s) within an FE are respectively primarily responsible for the process
are their respective department, while the medical adviser indicates to which organizational and
operational specifications the process must meet. In particular, they assess which process steps
must be taken to ensure adequate protection of personal data
with regard to health. The (team) manager is responsible for that inside
the FE the work instructions and advice drawn up by the medical adviser are complied with and the
employees in the FE comply with the Functional Unit Regulations and are also informed

of new laws and regulations or changes to existing laws and regulations. He also takes care of
signing the confidentiality agreement. [CONFIDENTIAL] finds a check of files
place, which also includes the processing of personal data, including personal data concerning the
health can be addressed. During these checks by the team leaders, the
medical advisors not always involved.

Work instructions and protocols are [CONFIDENTIAL] reviewed and tightened. The FG also tests and/or the [CONFIDENTIAL] periodical whether this is still in line with applicable laws and regulations. In in the event of changes, the work instructions and protocols will be updated by the medical advisers and team leaders and brought to the attention of the FEs.

During the interviews, Menzis indicated that in the absence of a medical adviser, the other medical advisers from the other FE(s). In that case, it is taken into account that the acting medical advisor is not an advisor who works for an FE who performs activities that are not may be combined with the activities of the FE to be observed (segregation of duties).

The Regulations FE include:

[CONFIDENTIAL]

The Regulations FE also state:

[CONFIDENTIAL]

At the request of the AP, Menzis has provided the most recent evaluation of the functioning of one of the functional units. [CONFIDENTIAL]

Menzis emphasizes that the medical adviser is not the only one who processes personal data health can handle. This would be unworkable. The law does not preclude declarations containing DBC codes are processed by others than medical advisers (read: a doctor). The FE employees who processing claims, however, are under the direction of the team manager and a medical adviser, Menzis has explained this. In concrete files containing the standard work protocols and instructions offer insufficient guidance, medical advisers provide advice on whether and which personal data health information are necessary and must be requested. A assessment of necessity is made at file level by the medical adviser if a file handler so requests. The advice of the medical advisor is according to the medical adviser in the file, for example by recording an e-mail from that medical advisor.

Judgement

-confidentiality

The AP notes in the first place that the medical advisors who manage the FEs are all doctors and
registered in accordance with the BIG Act (BIG registered). This places a duty of confidentiality on them
grounds of appeal.3 In the second place, the AP notes that all Menzis employees have a
duty of confidentiality under both a collective and an individual employment contract. FE-

3 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.

employees also sign an additional non-disclosure agreement. Applies to telephone employees
further that they must take the oath or affirmation.

In view of the foregoing, the AP comes to the conclusion that Menzis has complied with the provisions in
Article 21, first paragraph, opening words and under b, of the Wbp, read in conjunction with the second paragraph, now that
the
personal data concerning health are processed by persons acting on their behalf
profession (medical advisers) or under an agreement (Menzis employees).
to a duty of confidentiality.

-necessity requirement

Menzis has fulfilled the role of the medical adviser by assigning tasks to so-called
functional units in which personal data relating to health are processed under
responsibility of a medical advisor. The AP notes that the medical advisor has a role
in the advance preparation and interim adjustment of work instructions, step-by-step plans and safeguards
which employees must adhere to. In addition, medical advisors are available for
advice to FE employees and team leaders about concrete situations that deviate from the standard

work instructions. In the absence of a medical adviser, the other medical advisers take the FE(s)
of the absent adviser. The acting medical advisor is an advisor who does not work at
an FE that performs activities that are not allowed due to segregation of duties rules
combined with the activities of the FE to be observed.
In view of the foregoing, the AP comes to the conclusion that Menzis' chosen interpretation of
the role of the medical adviser has, in principle, sufficiently ensured that the assessment or interpretation
of the need 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 of the matter.
Superfluously, however, the AP notes the following. Monitoring compliance with the medical
work instructions drawn up by an advisor is largely assigned to the team managers, who do not themselves
are medical advisors. [CONFIDENTIAL] That in itself does not lead to a violation of the Wbp. The
AP points out, however, that the FE regulations drawn up by Menzis state that [CONFIDENTIAL].
To guarantee compliance with these principles, the AP advises Menzis to involve
the medical advisers in concrete cases, in particular when they deviate from the work instructions, te
intensify and record in files. In this way it becomes more clear how a
medical adviser is involved in the processing of personal data in daily practice
regarding health and the correct implementation thereof by employees of Menzis.
- 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 current investigation at Menzis, 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 Menzis is concerned with the medical

professional secrecy does not violate the Wbp.

10/12

Conclusions

Below is a conclusion for each part.

Code of Conduct and Privacy Policy

In view of the use of the Uniform Measures of ZN and the various own

policy documents, work processes and work instructions of Menzis, the AP is of the opinion that the few

fact that Menzis states on its website that it applies the code of conduct, which is now in place

rejected, not that Menzis is acting contrary to 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 Menzis, which should lead to a further investigation on this point.

Purpose limitation

The AP has not revealed any unlawful provisions by Menzis to third parties now that there is talk of

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

personal data concerning health. It has therefore not been shown that Menzis is used for this purpose

provides more personal data than is necessary and it has also not appeared that Menzis

provides personal data without a legal basis for doing so. The AP has

moreover, no instructions or signals are received that provide leads for another

conclusion.

Unauthorized access to personal data

Menzis has organized its corporate culture in such a way that only employees have access

may have access to personal data concerning health insofar as this is necessary for the

purpose for which the employees process the personal data. For example, by Menzis

stipulates that marketing employees are not allowed to share health-related personal data

process.

However, the investigation by the AP shows that marketing employees of Menzis do in fact have access to personal data concerning health. 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. Menzis therefore does not have sufficient technical means to guarantee this employees do not have access to personal data that is not necessary for the purpose for which they are processed. In that context, the AP points out that Menzis, for example, does not have any log files keeps track of access to personal data, including special personal data.

The foregoing leads to the conclusion that Menzis does not have suitable technological measures as referred to in Article 13 of the Wbp. The AP has underlying documents that show how a marketing campaign at Menzis is carried out, however, no indications were found for the conclusion that marketing employees actually collect personal data concerning health processing for a marketing campaign. However, this does not alter the conclusion that Article 13 of the Wbp is violated, because the technological measures that Menzis has taken are not appropriate.

Processors

It follows from the standard agreement and standard text that Menzis supervises correct compliance with the Wbp. Processors are thus explicitly informed of the special requirements that apply on the basis of the Wbp with regard to the processing of personal data relating to health. The AP concludes on the basis hereof that Menzis has complied with the obligations laid down in Article 14 of this point the Wbp in conjunction with Articles 12, 13 and 34a of the Wbp.

Doctor-patient confidentiality

The AP comes to the conclusion that Menzis does not act in violation of medical professional secrecy with the Wbp.

The AP concludes that personal data concerning health within Menzis are processed by persons subject to a duty of confidentiality by virtue of a profession (medical

advisers) as well as from an agreement (Menzis employees). In view of this, the AP comes to the conclusion that Menzis complies with the provisions of Article 21, first paragraph, opening lines and under b, of the Wbp, in read in conjunction with the second paragraph.

The AP also comes to the conclusion that Menzis, with its chosen interpretation of the role of the medical adviser has, in principle, sufficiently guaranteed 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. However, the AP Menzis recommends that the involvement of the medical advisers in specific cases be increased to intensify and record cases, especially when they deviate from the work instructions files.

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 Menzis, the AP did not have any leads to doubt the findings of the NZa on this point.