Findings Menzis

1. Code of Conduct and Privacy Policy

The Menzis Group includes the following risk bearers: 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 is valid for all legal entities mentioned.

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

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

Menzis 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) ZN's Material Control Protocol version 31 October 2016;

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.

Menzis also uses the following documents, partly 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) Privacy organization directive;

j) Procedure for the right of inspection and correction;

k) Right of opposition procedure;

l) Data processing notification procedure;

m) Procedure for misdirected medical records;

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 to report data breaches;

r) Information Security Policy;

s) Regulations for the establishment of the Functional Unit;

t) Confidentiality declarations (employment contract text, functional units, etc.).

u) Explanation of activities Compliance Function;

v) Thematic framework compliance 2017 version E&Y;

w) Submitter updating privacy policy, guidelines and procedures;

x) Logical Access Security Policy;

y) Menzis policy for segregation of duties 3.0;

z) Consent declaration SamenGezond;

aa) Contract guide working document;

bb) SCB Privacy and security measures;

cc) Article 15 AIV Privacy and Information Security.

Menzis has explained that it has a compliance control framework, on the basis of which it checks whether

appropriate implementation of privacy laws and policies. This system consists of a
detailed excel overview with a list of all components 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 conclude that
the standard has been met and how proof must be provided. The business units
of Menzis are periodically reviewed in full 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 case law.
The Data Protection Officer and the [CONFIDENTIAL] use a risk-based
and thematic approach to control the safeguarding of privacy. The entire organization is
[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, are
involved. This leads to a report with a score on whether these components are met. It
The latest research dates from [CONFIDENTIAL] and has to follow up on various points for attention in
[CONFIDENTIAL] guided.
With a view to the arrival of the General Data Protection Regulation (GDPR) on 25 May 2018
Menzis has drawn up a new control framework in collaboration with [CONFIDENTIAL], based on
of which the organization will be tested for compliance in the fourth quarter of 2017. anticipating
GDPR already carries out Privacy Impact Assessments for key business functions,
including the corporate functions [CONFIDENTIAL]
The basic principle of Menzis is that the use of personal data relating to health is only allowed
allowed for employees who need this data for their position and work and
if the necessity test is met (proportionality and subsidiarity requirements). This
principle is embedded in the culture of Menzis through its privacy policy, awareness
programs and the training program for new employees (e-learning) and the ongoing
training program for existing employees. All employees are required to

sign and comply with the nondisclosure agreement. Executives emphasize this at
repetition. Awareness for compliance with applicable laws and regulations regarding the protection of
personal data is encouraged as much as possible. Since [CONFIDENTIAL], around this
theme is organized annually, such as a 'Week for privacy', in which all employees

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

Rating

The Dutch Data Protection Authority (AP) concludes that Menzis does not exclusively use the
Code of Conduct, but also uses 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 tailored to the work of Menzis as a
health insurer. The AP also notes that Menzis has provided processes for the benefit of the
monitoring compliance with its privacy policy.

The AP also notes that Menzis ensures that the privacy policy is adapted to changes in
legislation and regulations and case law.

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

personal data. Through e-learning programs and theme weeks, among other things, the employees
van Menzis made as much as possible aware of how 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 set out in additional
documents, work processes and work instructions.
In view of the foregoing, the mere circumstance that Menzis states on its website that it
application of the code of conduct – which has meanwhile been rejected, not already that Menzis acts contrary to
with the Personal Data Protection Act (Wbp).
2. Digital declaration without diagnostic information
Following a decision by the CBB that health insurers must provide for a privacy regulation
on the basis of which mental health care patients should be able to declare information without stating a diagnosis,1
In March 2012, the NZa provided a scheme. In connection with this, Menzis has
insurance conditions since 2014 the following text has been included as standard:
! NB
If you do not want the diagnosis code to be stated on the claim, but you still want to submit the claim for reimbursement,
If you want to be eligible, a statement is required prior to or at the latest with the first declaration. You must work with
your practitioner to sign a statement and send it to Menzis. This statement can be found at
1 CBB August 2, 2010, ECLI:NL:CBB:2010:BN3056.

www.menzis.nl/fees.
Menzis has also explained that, as a result of the NZa's investigation in 2016, it
of entering standard letters ensures that in case an insured makes use of
a privacy statement, you are no longer asked for the integral referral letter or treatment plan.
Rating
For the way in which Menzis handles privacy statements and requesting information from the
insured persons, the AP refers to the NZa study from 20162, 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 Menzis that will lead to further details

research on this point.

3. Target binding

-marketing

Menzis indicates that it does not process personal health data for

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

Under this program, personal data relating to health will only be processed

express permission of the participant. If the participant withdraws his/her consent, then

the program is ended.

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

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

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

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

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

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

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

of regular personal data such as name, address, e-mail and telephone details, designation male 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 the recipient has been selected on the basis of personal health data.

-exception to target limitation

To the extent that the Code of Conduct allows for an exception to the purpose limitation principle,

make, Menzis indicates that it does not actively use this option laid down in Article

3.13 of the Code of Conduct.

Menzis has argued that only in the event of a report or when they have a

receives a claim from the police or judicial authorities, or the tax authorities, applies Article 3.13 of

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

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

provision of personal data is subject to the Uniform Measure 8 of ZN. A

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

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

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

[CONFIDENTIAL]

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,

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

prior to that, are not based on personal health data.

The AP has established 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 virtually identical to Article 43 of the

Wbp.

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

Menzis provides personal data. This applies in particular to cases of fraud. The premise of

Menzis is that, in principle, no personal data relating to health will be collected 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 benefits are

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

For the provision of personal data (relating to health) to the police, the judiciary, the
The tax authorities (and statutory supervisors) have a legal 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 using 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
In the opinion of the AP, a sufficiently specific elaboration of this article for health insurers. From the
underlying information has not emerged of any unlawful provision by Menzis 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. Therefore, it has not been shown that
Menzis provides more personal data for this purpose than is necessary and has not been shown either
that Menzis provides personal data without there being a legal basis for this. the AP
furthermore, has not received any indications or signals that offer leads for another
conclusion.

4. Unauthorized access to personal data

[CONFIDENTIAL]

Rating

- authorization policy general

[CONFIDENTIAL]

- authorizations employees marketing department

[CONFIDENTIAL]

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

employees adhere to it in practice. [CONFIDENTIAL]

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

relating to health 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 relating to health insofar as this is necessary for the

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

It has been established that marketing employees are not allowed to provide personal data relating to health

process.

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

have access to personal data relating to health. 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.

Menzis therefore does not have sufficient technical means to ensure that:

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 appropriate technological measures

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

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

conclusion that marketing employees actually have personal data relating to health

process for a marketing campaign. However, this does not detract from the conclusion that Article 13 of the Wbp is

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

5. Editors

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 shaped. The standard texts and contracts that Menzis uses are

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

Rating

The AP has both the standard texts and contracts as a completed version of a

processing agreement. The AP concludes from this that those agreements provide for a

translation of the obligations arising from the Personal Data Protection Act and the Code of Conduct for the processors of Menzis and

that this concerns 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 regarding 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 so

explicitly referred to the special requirements that apply under the Wbp with regard to processing

of personal health data. On this basis, the AP concludes that Menzis

on this point, the obligations laid down in Article 14 of the Wbp in conjunction with . have been met

Articles 12, 13 and 34a of the Wbp.

6. Medical professional secrecy

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

counselor. [CONFIDENTIAL]

With regard to confidentiality, Menzis has explained the following.

FE employees are required to sign a nondisclosure agreement upon employment. The

confidentiality statement is part of the individual employment contracts of Menzis

employees and these employees are also on the basis of the applicable collective labor agreement

(cao) held to secrecy. Employees who work in an FE sign in connection with the

processing personal data relating to health, in addition, an additional FE-

nondisclosure agreement. Menzis employees who have customer contact must also take an oath or

make a promise that they will keep secret what is entrusted to them over the phone. In

In addition to these measures, annual privacy awareness programs are carried out by means of

of e-learning, presentations in work meetings by the Data Protection Officer and/or

the Compliance officer, mystery guest visits and video messages from the CEO.

Menzis has explained the following about the role of the medical advisor.

The medical advisor broadly determines whether and which personal data concerning health

are necessary and must, for example, be requested from a healthcare provider. As much as possible

standard instructions and work processes are used in which the protection of personal data

are embedded. These instructions and work processes have been drawn up in part by the medical advisor and are

at least [CONFIDENTIAL] reviewed and updated. This will be done sooner if necessary.

Menzis further explained during the interview that when requested to do so, the

performing a detail check at file level at a healthcare provider on site until the work is completed

of a medical advisor.

The (team) manager(s) within an FE are respectively primarily responsible for the process at

their respective departments, while the medical advisor indicates to which organizational and

operational specifications the process must meet. In particular, they assess which process steps

should be taken to ensure adequate protection of personal data with

with regard to health. The (team) manager is responsible for ensuring that

the FE the work instructions and advice drawn up by the medical advisor 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 file check

place, which also includes the processing of personal data, including personal data relating to the

health can be addressed. Incidentally, during these checks by the team leaders, the

medical advisors are not always involved.

Work instructions and protocols are viewed and tightened up [CONFIDENTIAL]. The FG . also tests
and/or the [CONFIDENTIAL] periodically or whether this is still in line with applicable laws and regulations. In
In the event of changes, the work instructions and protocols are reviewed 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 advisor, the other
observe medical advisers from the other FE(s). In that case, it is taken into account that the
acting medical adviser is not an adviser who works for an FE who performs activities that are not
may be combined with the activities of the FE to be observed (separation of duties).
The FE Regulations include:
[CONFIDENTIAL]
The FE Regulations 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 advisor is not the only one who can provide personal data regarding the
health can handle. This would be unworkable. The law does not exclude that declarations containing
DBC codes are processed by parties other than medical advisers (read: a doctor). The FE employees who
however, handling claims are under the direction of the team manager and a medical advisor,
this is how Menzis explained. In concrete files in which the standard work protocols and instructions
provide insufficient guidance, medical advisers provide advice on whether and which personal data
health-related are necessary and must be requested. A
necessity assessment is made at file level by the medical advisor if a
file handler so requests. The advice of the medical advisor is according to the medical
advisor included in the file, for example by recording an e-mail from that person
medical advisor.
Rating

-confidentiality

In the first place, the AP notes that the medical advisors who manage the FEs are all doctors and registered in accordance with the BIG Act (BIG-registered). They are therefore subject to a duty of confidentiality on grounds of appeal.3 Secondly, the AP establishes that all Menzis employees have a duty of confidentiality on the basis of both a collective and an individual employment contract. FE-

3 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.

employees also sign an additional confidentiality 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 of Article 21, first paragraph, preamble and under b, of the Wbp, read in conjunction with the second paragraph, now the personal data relating to health are processed by persons who, by virtue of their profession (medical advisers) or subject to an agreement (Menzis employees) to a duty of confidentiality.

-necessity requirement

Menzis has fleshed out the role of the medical advisor 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 pre-drafting and interim adjustment of work instructions, step-by-step plans and guarantees that employees must adhere to. In addition, the 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 advisor, the other medical advisors will take the FE(s) of the absent advisor. The acting medical advisor is an advisor who does not work for

an FE who carries out work that may not be performed due to segregation of duties
combined with the work of the FE to be observed.
In view of the foregoing, the AP comes to the conclusion that Menzis, with its chosen interpretation of
the role of the medical adviser has in principle sufficiently ensured that the assessment or interpretation
of the need to process personal data relating to health in accordance with
under the Wbp and the Zvw is carried out by someone with sufficient (medical) knowledge.
Superfluously, however, the AP notes the following. Supervision of compliance with the medical
work instructions drawn up by a consultant is largely assigned to the team managers, who themselves do not have any
are medical advisers. [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].
In order to guarantee compliance with these principles, the Menzis AP recommends that the involvement of
the medical advisers in specific cases, in particular when they deviate from the work instructions, to
intensify and record in files. In this way it becomes clearer how a
medical advisor is involved in the processing of personal data in daily practice
concerning health and its correct implementation by Menzis employees.
-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 Menzis 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 with regard to the medical
professional secrecy does not violate the Wbp.

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 proprietary

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

fact that Menzis states on its website that it applies the code of conduct, which has now been implemented

disapproved, not already that Menzis acts 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

van Menzis that should lead to further investigation on this point.

Target binding

The AP has not revealed any unlawful provisions by Menzis 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. It has therefore not been shown that Menzis is used for this purpose

provides more personal data than is necessary and it has not been shown that Menzis

provide personal data without there being a legal basis for this. The AP has

furthermore, do not receive any indications or signals that offer 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 relating to health insofar as this is necessary for the

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

It has been established that marketing employees are not allowed to provide personal data relating to health

process.

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

have access to personal data relating to health. 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.
Menzis therefore does not have sufficient technical means to ensure that:
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 appropriate technological measures
as referred to in Article 13 of the Wbp. The AP has from underlying documents that show how
a marketing campaign is carried out at Menzis, incidentally, no indications were found for the
conclusion that marketing employees actually have personal data relating to health
process for a marketing campaign. However, this does not detract from the conclusion that Article 13 of the Wbp is
because the technological measures that Menzis has taken are not appropriate.

Editors
It follows from the standard agreement and standard text that Menzis supervises correct compliance with the
Wbp. Processors are thus explicitly pointed out to the special requirements that apply under the Wbp at
with regard to the processing of personal data relating to health. The AP concludes on the basis of
of this that Menzis has complied with 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 Menzis 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 Menzis
processed by persons who are subject to a duty of confidentiality by virtue of a profession (medical
advisors) 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 words 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 relating to health in accordance with the Wbp and the Zvw is carried out by someone with sufficient (medical) knowledge. However, the AP Menzis does recommend in this regard that the involvement of the medical advisers in concrete cases, especially when they deviate from the work instructions, and to record them in files.

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 Menzis, the AP has not leads were found to doubt the findings of the NZa on this point.