Registered

Coöperatie Menzis U.A.

Chairman of the Board of Directors

Mr R. Wenselaar

PO Box 75000

7500 CC Enschede

Date

February 15, 2018

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

070 8888 500

Subject

Order subject to periodic penalty payments and final findings

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authoritypersonal data.nl

Your feature

20171025/EB/jd

Dear Mr Wenselaar,

Below you will find the decision of the Dutch Data Protection Authority (AP) to impose an order under penalty to Coöperatie Menzis U.A. (Menzis). This decision is part of the new decision of today to the objection of Civil Rights Association Vrijbit (Vrijbit). This new decision on objection is

taken after the investigation carried out by the AP in response to the interim ruling of the Midden Nederland District Court (the District Court) of 7 July 2017, ECLI:NL:RBMNE:2017:3421 (the interim statement). This case started with an enforcement request that Vrijbit submitted to the Board protection of personal data (CBP).

Vrijbit's enforcement request relates to the way in which Dutch health insurers apply currently process personal data relating to health. According to Vrijbit, this method is in conflict with the Personal Data Protection Act (Wbp), the Charter of Fundamental Rights of the European Union (the Charter) and Article 8 of the Convention on Human and Human Rights fundamental freedoms (ECHR). In summary, Vrijbit lays the basis for this that health insurers still always work in accordance with the Code of Conduct for the Processing of Personal Data Health Insurers (the code of conduct),

while the AP has withheld its approval of that code of conduct as a result of a judgment of the court of Amsterdam from 2013.1

The course of the procedure between Vrijbit and the AP, the legal framework, the ruling of the District Court of Amsterdam, the interim ruling, the original decision on the objection of 1 June 2016, the design of the investigation and the course of the investigation are set out in the new decision op objection. The AP refers to this for the sake of brevity.

1 Court of Amsterdam 13 November 2013, ECLI:NL:RBAMS:2013:7480.

Date

February 15, 2018

Our reference

[CONFIDENTIAL]

Findings

The AP's findings are appended to this decision to impose the order subject to periodic penalty payments attached. First of all, the code of conduct and the privacy policy applied by Menzis are discussed order (1). Subsequently, the aspects digital declaration without diagnosis information (2), purpose limitation (3), unauthorized access to personal data (4), processors (5) and medical professional secrecy (6).

Offence

In the findings, the AP comes to the conclusion that Menzis violates Article 13 of the Wbp. The AP has in observed the following in that context:

- 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, through Menzis has laid down that marketing employees do not store any personal data concerning health allowed to 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 can be regarded as the processing of personal data.
- Menzis therefore does not have sufficient technical means to guarantee 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 a keeps log files about access to personal data, including special personal data.
- The foregoing leads to the conclusion that Menzis does not have suitable technological equipment measures as referred to in Article 13 of the Wbp. The AP has that from underlying documents

not showing how a marketing campaign is carried out at Menzis

found indications for the conclusion that marketing employees actually

process personal data concerning health for a marketing campaign. However, it does

does not alter the conclusion that Article 13 of the Wbp has been violated because of the technological measures

that Menzis has affected are not appropriate.

Duty of principle to enforce

From Article 65 of the Wbp, viewed in conjunction with Article 5:32, first paragraph, of the General Act

administrative law (Awb) follows that the AP is authorized to impose an order subject to periodic penalty payments in the event

of a violation

of Article 13 of the Wbp.

Pursuant to Article 5:2, first paragraph, opening words and under b, of the Awb, the order subject to periodic penalty payments

is aimed at

ending the established violation and preventing recurrence.

In view of the public interest served by enforcement, the AP will, in the event of a violation of

a statutory provision, as a rule, must make use of its enforcement powers.

Special circumstances in connection with which enforcement action must be waived

not occur in this case.

Date

February 15, 2018

Our reference

[CONFIDENTIAL]

Order subject to periodic penalty payments and grace period

The AP orders Menzis to set up its system in such a way that unauthorized access to

personal data is prevented.

The authorization matrix and accompanying documents in which they are the logical

To ensure adequate technological control systems on the basis of which it guarantees

To this end, it must in any case:

1.

access security of its systems must be adjusted. This

documents should be amended or re-drafted in such a way that it clearly follows

what access rights employees have. The authorization matrix serves as a clear overview

of the authorizations and view roles associated with a function or role by means of

including an unambiguous use of terminology. Menzis must record for this

what function or role the processing of personal data concerning health is necessary

is and for what purpose and to review this document with revised business judgments if necessary

to fit. Furthermore, the authorizations of Menzis employees are permanently submitted in fact

to be brought into agreement.

2.

that employees only have access to special personal data, including

personal data concerning health, when such access is necessary for the

activities of an employee. In any case, this concerns logging of access and

changes, so that - whether or not as a result of incidents - it can be checked whether

employees have gained access while access to this data is not necessary

for their activities. This also means that the authorizations must be periodically

checked and immediately adjusted if an inspection shows that an employee is at

is wrongly authorized to access personal data, including

personal data concerning health.

3.

takes place at least once every six months – by the Data Protection Officer and

the Compliance officer(s) to the management showing whether any incidents have occurred and so on

yes, what measures have been taken:

a.

b.

Menzis must also provide periodic written feedback – which is at least

with regard to what is stated under 1;

with regard to what is stated under 2.

6

7

-benefit period and penalty amount with regard to parts 2 and 3b

In view of what Menzis has put forward about its wish to set up its system in such a way that

technically and largely automated it is ensured that employees do not have access to more

personal data than is necessary for their work, the AP connects to part 2 and

part 3b of this charge has a grace period ending December 31, 2018.

If Menzis does not meet the obligation before the end of the beneficiary period referred to under 6,

she forfeits a penalty. The AP sets the amount of this penalty at an amount of

€ 150,000.00 for each (whole) week, after the last day of the set term, on which

Menzis fails to comply with part 2 and part 3b of the order, up to a maximum of € 750,000.00.

Considering the fact that the penalty should be an incentive to comply with the order, the amount of the turnover

Date

February 15, 2018

Our reference

[CONFIDENTIAL]

of Menzis, the large number of insured persons and the seriousness of the violation, the AP is aware of this

coercion appropriate.

-benefit period and amount of penalty with regard to parts 1 and 3a

With regard to part 1. of this burden, the AP is of the opinion that with its implementation less efforts are involved. The AP therefore connects to part 1 and part 3a of the load one beneficiary period ending May 26, 2018.

If Menzis does not meet the obligation before the end of the beneficiary period stated under 0, she forfeits a penalty. The AP sets the amount of this penalty at an amount of € 50,000.00 for each (entire) week, after the last day of the set term, on which Menzis fails to pay part 1 and part 3a of the burden, up to a maximum of € 250,000.00.

Considering the fact that the penalty should be an incentive to comply with the order, the amount of the turnover of Menzis, the large number of insured persons and the seriousness of the violation, the AP is aware of this coercion appropriate.

-interim report

The AP advises Menzis to communicate once per quarter on the basis of a concrete schedule to do to the AP about the progress of the measures it is taking to comply with the imposed load.

-post-check

The AP requests Menzis to provide documentary evidence to the AP in good time before the end of the beneficiary period evidencing that the payment has been made on time and in full. Timely submission of documentary evidence does not alter the fact that the AP is authorized to conduct an investigation, including an investigation on site, if appropriate.

Explanation of the burden

The AP notes the following by way of explanation.

In the document 'CBP Guidelines. Security of personal data' (Stcrt. 2013, 5174, hereinafter also: de guidelines) the question of when security measures are 'appropriate' in the sense of Article 13 of the Wbp. The guidelines make it clear that for that assessment first of all the reliability requirements to be set must be taken into account. This must be based on the nature of the data to be protected is determined what an appropriate level of protection is. The nature of the

personal data is important here. Also the amount of processed personal data per person and

the purpose for which the personal data are processed must be taken into account.

In this case it concerns the processing of data concerning health, being special

personal data. This means that the consequences of an unlawful processing of that data,

can be serious for those involved. As a result, for the processing of personal data

Menzis requires a high level of security.

8

9

10

11

12

13

14

Date

February 15, 2018

Our reference

[CONFIDENTIAL]

15

16

After the reliability requirements have been established, the responsible party must make appropriate

take security measures that guarantee that the reliability requirements are met, so

is in the guidelines. Security standards provide guidance when actually meeting

appropriate measures to cover the risks. A very widely used security standard is the

Code for Information Security, NEN-ISO/IEC 27002+C1(2014)+C2 (2015). Here are specifics

security measures included. Security standards provide guidance during the actual encounter

of appropriate measures to cover the risks. What security standards for a particular
processing are relevant and which security measures based on these security standards
should be taken, however, must be determined on a case-by-case basis.
The Code for Information Security mentions the following relevant measures in this context:
9.4.1 Information Access Restrictions
Access to information and system functions of applications should be restricted in accordance with it
access security policy.
12.4.1 Record events
Event logs that record user activities, exceptions, and information security events
record, should be made, kept and regularly reviewed.
17 Irrespective of the structure of the access security policy, the nature of the
personal data that a health insurer such as Menzis processes and the extent of that processing, that is
at least log files are kept in such a way that at least a reactive check of
the log files is possible. In particular, the AP is concerned that actions in the form of
consultations or changes in the systems that employees are authorized to access
(special) personal data are not logged, as a result of which access to that is controlled
data – for example as a result of incidents – is currently not possible.
18 As noted above, the AP found during the investigation that marketing employees
of Menzis actually have access to personal data concerning health, while Menzis
it has been established that this is not the intention. In its response to the intention to enforce, Menzis has stated the
acknowledged the correctness of these findings and declared to be committed to the opinion of the AP that this
leads to a violation of Article 13 of the Wbp. Menzis has stated that it will receive the
to take necessary action to end the violation. She has a plan for this with the AP
of the measures it intends to take. This planning seems realistic to the AP.
The AP therefore has the aforementioned beneficiary periods for the various parts of
the order subject to periodic penalty payments is aligned with Menzis' planning.

Date

February 15, 2018

Our reference

[CONFIDENTIAL]

19

For the information of the parties

Today's decision on objection with reference z2016-12335 and the present decision imposing

the order subject to periodic penalty payments and together form the AP's decision on Vrijbit's objection. Against this

decision is subject to appeal to the court.

A copy of this letter will be sent to the Data Protection Officer of

Menzis [CONFIDENTIAL].

Yours faithfully,

Authority for Personal Data,

e.g.

Mr. A. Wolfsen

Chair

Remedy

If you do not agree with this decision, you can within six weeks of the date of sending it

decision pursuant to the General Administrative Law Act to file a notice of appeal with the court

Central Netherlands, where this procedure is already pending. You must enclose a copy of this decision

send. Submitting a notice of appeal does not suspend the operation of this decision.