

Registered mail

Cooperative Menzis U.A.

Chairman of the Board

Mr. R. Wenselaar

PO Box 75000

7500 KC Enschede

Date

February 15, 2018

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

070 8888 500

Topic

Order subject to penalty 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

[authority data.nl](http://authority.data.nl)

Your feature

20171025/Board/jd

Dear Mr. Wisher,

Below you will find the decision of the Dutch Data Protection Authority (AP) to impose an order under

penalty to Cooperative Menzis U.A. (Menzis). This decision is part of the new decision

from today on the objection of the Civil Rights Association Vrijbit (Vrijbit). This new decision on objection is

taken after the investigation carried out by the AP following the interim ruling of the Midden Nederland court (the court) dated 7 July 2017, ECLI:NL:RBMNE:2017:3421 (de interlude). This case was started with an enforcement request that Vrijbit submitted to the College protection of personal data (CBP).

Vrijbit's enforcement request relates to the way in which Dutch health insurers are currently processing personal data relating to health. According to Vrijbit, this method is in violation of 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 Rights and the fundamental freedoms (ECHR). Vrijbit, in summary, underlies this that health insurers are still always work in accordance with the Code of Conduct for the Processing of Personal Data for Healthcare Insurers (the code of conduct), while the AP still withheld its approval of that code of conduct as a result of a judgment of the Amsterdam District Court from 2013.<sup>1</sup>

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

<sup>1</sup> Amsterdam District Court 13 November 2013, ECLI:NL:RBAMS:2013:7480.

1

Date

February 15, 2018

Our reference

[CONFIDENTIAL]

1

2

3

## Findings

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

## Offence

In its findings, the AP concludes that Menzis violates Article 13 of the Wbp. The AP has in that framework noted the following:

- 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, by Menzis has established that marketing employees do not receive personal data regarding health allowed to 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, pursuant to Article 1, opening words and under b, of the Wbp can 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 maintain log files about 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 from underlying documents that

show how a marketing campaign is carried out at Menzis, by the way, no found indications for the conclusion that marketing staff actually processing personal data relating to health for a marketing campaign. However, that does does not detract from the conclusion that Article 13 of the Wbp has been violated, because the technological measures that Menzis has affected are not appropriate.

#### Principle of enforcement

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 a penalty in the event of 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 a penalty is aimed at the terminating the detected violation and preventing repetition.

In view of the public interest served by enforcement, in the event of a violation of a statutory provision, as a rule, have to make use of its enforcement powers.

Special circumstances in connection with which enforcement action must be waived, do not occur in this case.

2/6

Date

February 15, 2018

Our reference

[CONFIDENTIAL]

Order subject to penalty and beneficiary period

The AP orders Menzis to set up its system in such a way that unauthorized access to personal data is prevented.

5

The authorization matrix and associated documents in which they provide the logical

Ensure adequate technological control systems on the basis of which it ensures

To that end, it must in any case:

1.

access security of its systems must be adjusted. This one documents must be adapted or redrafted in such a way that it clearly follows what access rights employees have. The authorization matrix should provide an insightful overview provide the authorizations and consult roles associated with a position or role by means of including an unambiguous use of terminology. Menzis must record this for: which function or role the processing of personal data concerning health is necessary is and for what purpose and this document is subject to revised business insights, if necessary to suit. Furthermore, the authorizations of Menzis employees must therefore be permanently to be brought into agreement.

2.

that employees only have access to special personal data, including personal data relating to health, where such access is necessary for the work 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 obtained access while access to this data is not necessary for their work. This also means that the authorizations must be periodically checked and adjusted without delay if an audit shows that an employee is at least has been 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, which shows whether incidents have occurred and so yes, which measures have been taken:

a.

b.

Menzis must also provide periodic written feedback – which is

with regard to the aforementioned under 1;

with regard to the above mentioned under 2.

6

7

- beneficiary period and amount of penalty 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 a beneficiary period that ends on December 31, 2018.

If Menzis does not meet the payment 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 (entire) week, after the end of the last day of the set term, on which

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

In view of the fact that the penalty must be an incentive to comply with the order, the amount of the turnover,

3/6

Date

February 15, 2018

Our reference

[CONFIDENTIAL]

van Menzis, the large number of insured persons and the seriousness of the violation, the AP considers to be aware of this penalty appropriate.

- beneficiary 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 the implementation thereof less

efforts are involved. The AP therefore attaches to part 1 and part 3a of the charge a

beneficiary period ending on 26 May 2018.

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

In view of the fact that the penalty must be an incentive to comply with the order, the amount of the turnover, van Menzis, the large number of insured persons and the seriousness of the violation, the AP considers to be aware of this penalty appropriate.

-interim report

The AP advises Menzis to make a statement on the basis of a concrete planning – once a quarter to inform the AP about the progress of the measures it is taking to comply with the imposed burden.

-post-check

The AP requests Menzis to submit supporting documents to the AP in good time before the end of the beneficiary period send proof that the charge has been paid in full and on time. The 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 deemed appropriate.

Explanation of the load

By way of explanation, the AP notes the following.

In the document 'CBP Guidelines. Security of personal data' (Government Gazette 2013, 5174, hereinafter also: de guidelines) the question of when security measures are 'appropriate' within the meaning 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 considered. This must be done on the basis of 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 relating to health, i.e. 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 requires a high security level by Menzis.

8

9

10

11

12

13

14

4/6

Date

February 15, 2018

Our reference

[CONFIDENTIAL]

15

16

After establishing the reliability requirements, the responsible party must take security measures to ensure that the reliability requirements are met, such as is in the guidelines. Security standards provide guidance when actually taking 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). In this are concrete security measures included. Security standards provide guidance during the actual encounter appropriate measures to cover the risks. Which security standards for a particular processing are relevant and which security measures based on these security standards



should be taken, however, should be determined on a case-by-case basis.

The Code for Information Security lists the following relevant measures in this regard:

#### 9.4.1 Restricting access to information

Access to information and system functions of applications should be restricted in accordance with the access security policy.

#### 12.4.1 Log events

Event logs that record user activities, exceptions, and information security events should be created, stored and regularly reviewed.

17 Irrespective of the design of the access security policy, the nature of the personal data that a health insurer such as Menzis processes and the scope of that processing, which is at least 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 with acts in the form of consultations or changes in the systems to which employees are authorized with regard to (special) personal data are not logged, as a result of which a check on access to that data 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 regarding health, while Menzis it has been established that this is not the intention. In its response to the intention to enforce, Menzis has correctness of these findings and declares to commit to the judgment of the AP that this leads to a violation of Article 13 of the Wbp. Menzis has stated that it will receive the take the necessary steps to end the violation. The AP has a plan for this of the measures it intends to take. This planning seems realistic to the AP.

The AP has therefore set the aforementioned favorable terms for the various parts of the order subject to periodic penalty payments is geared to Menzis' planning.

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 to impose the order subject to periodic penalty payments and together they form the decision of the AP 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 Personal Data,

w.g.

mr. A. Wolfsen

Chair

Remedy

If you do not agree with this decision, you can return it within six weeks of the date of dispatch of the decision to submit a notice of appeal to the court pursuant to the General Administrative Law Act

Central Netherlands, where these proceedings are already pending. You must enclose a copy of this decision send. Submitting a notice of appeal does not suspend the effect of this decision.

6/6