Registered

Coöperatie VGZ U.A.

The Chairman of the Board of Directors

Mr R. Kliphuis

PO Box 5040

6802 EA ARNHEM

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

Dear Mr Cliffhouse,

Below you will find the decision of the Dutch Data Protection Authority (AP) to impose an order under periodic penalty payment to Coöperatie VGZ U.A. (VGZ). This decision is part of the new decision of today on 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 VGZ 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).

In its findings, the AP concludes that VGZ violates Article 13 of the Wbp. The AP has in observed the following in that context:

- VGZ 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. So is, among other things established by VGZ that marketing employees do not store any personal data concerning the handle health.
- However, the AP's investigation shows that a number of employees of the Customer and Brand partners of VGZ actually have access to personal data concerning health, while this is not necessary for their work. Being able to consult personal data can be regarded as the processing of personal data.
- VGZ therefore does not have sufficient technical means to guarantee this employees have not had access to personal data that is not necessary for the purpose for which they are processed. In this context, the AP further points out that VGZ has no keeps log files about access to special personal data.
- The foregoing leads to the conclusion that VGZ does not have suitable technological facilities measures as referred to in Article 13 of the Wbp;
- In the documents submitted, the AP has indicated how a marketing campaign at VGZ is carried out, however, no indications were found for the conclusion that marketing employees actually process personal data concerning health

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

violated, because the technological measures taken by VGZ 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.

Order subject to periodic penalty payments and grace period

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

personal data is prevented.

5

The authorizations and viewing roles used by VGZ for logical access security

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

To this end, it must in any case:

1.

systems of the Customer and Brand Partners department need to be adjusted, more

specifically for the employees listed in Confidential Annex 1. These authorizations and

consultation roles of the aforementioned VGZ employees must be adjusted in such a way that

that these employees actually no longer have access to personal data, including

personal data concerning health, when the processing of this personal data

not necessary for their work.

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.

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.

with regard to what is stated under 1;

with regard to what is stated under 2.

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

6

7

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

In view of what VGZ 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 VGZ 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 every (whole) week, after the last day of the set term, on which VGZ 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 of VGZ, the large number of insured persons and the seriousness of the violation, the AP considers it to be 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 VGZ does not meet the obligation before the end of the beneficiary period referred to under 8, she forfeits a penalty. The AP sets the amount of this penalty at an amount of € 50,000.00 for each (whole) week, after the last day of the set term, on which VGZ fails to comply 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 VGZ, the large number of insured persons and the seriousness of the violation, the AP considers it to be aware of this

coercion appropriate.

-interim report

The AP advises VGZ to make a statement once per quarter on the basis of a concrete schedule

inform the AP about the progress of the measures it is taking to comply with the

imposed load.

-post-check

The AP requests VGZ 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

VGZ requires a high level of security.

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

8

9

10

11

12

13

14

15

Date

February 15, 2018

Our reference

[CONFIDENTIAL]

16

17

18

19

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.

Irrespective of the design of the access security policy, the nature of the

personal data that a health insurer such as VGZ processes and the extent of that processing, that ten

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.

As noted above, the AP found during the investigation that a number of employees

of the Customer and Brand Partners department have authorizations that give access to personal data

concerning health, while this is not necessary for their work. VGZ has in her

response to the intention to enforce acknowledged the correctness of this finding. VGZ has stated that

it has taken corrective measures, as a result of which the wrongful access has ended. Already

because this statement is not supported by evidence, the AP sees no reason to waive this point

of enforcement.

VGZ has also put forward that the AP in its provisional findings wrongly made a

has made a link between logging and preventing unauthorized access to

personal data. In response to this, the AP points out the following. The AP already has this under 17

explained that and why keeping log files for a health insurer such as VGZ is a

necessary measure to ensure an appropriate level of security. This applies all the more to VGZ,

now that she has an access security policy that involves working with an authorization matrix

per officer. This entails the risk that the authorizations actually granted will not be valid over time

no longer correspond to the authorizations that are strictly necessary for the activities of the

relevant employee.

Although the AP has not established that other VGZ employees have authorizations and

roles that enable more far-reaching access to (special) personal data than necessary

however, the AP VGZ has recommended that the authorization policy be developed in such a way that if

The main rule is that for each function (group) it is determined which roles and authorizations are to be exercised

of that function are necessary.

20 With regard to the beneficiary period, VGZ has proposed that the necessary

measures to meet the burden. VGZ has stated that it is dependent on this

third parties. VGZ has not made this clear on the basis of a substantiated planning. Seen

the seriousness of the violation and the measures to be taken in the opinion of the AP, the AP deems the above

periods stated under 6 and 8 are appropriate and reasonable.

What VGZ put forward on this point in its response to the intention to enforce

In view of the foregoing, this is no reason for the AP to refrain from taking enforcement action.

21

For the information of the parties

22 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

VGZ, [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 from 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.