Confidential/Registered

OLVG Foundation

Attn. mr prof. dr. M.A.A.J. Van den Bosch

Chairman of the Board of Directors

PO Box 95500

1090 HM Amsterdam

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Subject

Decision to impose an administrative fine

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 van den Bosch,

The Dutch Data Protection Authority (AP) has decided to impose an administrative fine on Stichting OLVG (OLVG).

of €440,000 because OLVG has not met the requirement of two-factor authentication

and reviewing log files regularly. OLVG therefore has insufficient suitable ones

measures taken as referred to in Article 32(1) of the General Regulation

Data Protection (GDPR).

The decision is explained in more detail below. Chapter 1 is an introduction and Chapter 2 describes it

legal framework. In chapter 3, the DPA assesses the processing responsibility and the violation.

The (amount of the) administrative fine is elaborated in chapter 4 and chapter 5 contains the operative part and the remedies clause.

1

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

1 Introduction

1.1 Legal entities involved and reason for the investigation

OLVG is a foundation that has its registered office at Oosterpark 9, in Amsterdam. OLVG is registered in the trade register of the Chamber of Commerce under number 41199082. OLVG is a top clinical teaching hospital in Amsterdam with two main locations in Amsterdam East and West. OLVG offers medical care to approximately 500,000 patients annually. In 2018, OLVG had 5890 salaried employees, of which 4274 in patient-related positions.1

The AP has received two data breach reports from the OLVG Foundation about access by employees and working students in electronic patient records. As a result of these data breach reports, the AP initiated an ex officio investigation into compliance by OLVG with Article 32, first paragraph, of the GDPR by among other things, to investigate security aspects such as authentication and checking the logging.

1.2 Process flow

In a letter dated 17 April 2019, the AP announced the investigation and asked questions to OLVG. This questions were answered by OLVG by letter dated 3 May 2019.

On May 22, 2019, five AP supervisors conducted an on-site investigation at OLVG, location East, at Oosterpark 9 in Amsterdam. During this investigation, the hospital information system is up various moments and parts demonstrated and viewed. There are also oral ones statements taken from members of the Board of Directors and from various employees of OLVG.

The AP sent the report with findings to OLVG on February 10, 2020. By letter dated 17 February
In 2020, the AP sent OLVG an intention to enforce. Also with this letter
given the AP the opportunity, OLVG has written on March 27, 2020 and orally on June 25, 2020
expressed its views on this intention and the report on which it is based.

2. Legal framework

2.1 Scope GDPR

Pursuant to Article 2, paragraph 1, of the GDPR, this Regulation applies to the whole or in part
automated processing, as well as to the processing of personal data contained in a file
included or intended to be included therein.

Pursuant to Article 3, paragraph 1, of the GDPR, this regulation applies to the processing of

1 Annual Report 2018 OLVG, p. 5-6.

personal data in the context of the activities of an establishment of a
controller or a processor in the Union, whether or not the processing takes place in the Union
does not take place.

Pursuant to Article 4 of the GDPR, for the purposes of this Regulation:

1. “Personal Data”: any information relating to an identified or identifiable natural person
(“the data subject”); […].

2. “Processing”: an operation or set of operations relating to personal data or
a set of personal data, whether or not carried out by automated processes […].

7. “Controller”: a […] legal entity that, alone or jointly with others, achieves the purpose of
and determines the means of processing personal data; […].

15. “Health Data” means personal data related to the physical or mental

health of a natural person, including data on health services provided

providing information about his health status.

2.2 Security Obligation

Pursuant to Article 32, paragraph 1, of the GDPR, the controller, taking into account

the state of the art, the implementation costs, as well as the nature, scope, context and the

processing purposes and the varying likelihood and severity of risks to the rights and

liberties of persons, appropriate technical and organizational measures to prevent one at risk

to ensure an appropriate level of security […].

Pursuant to the second paragraph, the assessment of the appropriate security level takes particular account

into account the risks of processing, in particular as a result of the destruction, loss, alteration or deletion

unauthorized disclosure of or unauthorized access to transmitted, stored or otherwise

processed data, either accidentally or unlawfully.

2.3 Administrative fine

Pursuant to Article 58, paragraph 2, opening words and under i, in conjunction with Article 83, paragraph 4, opening words and

under

a, of the AVG and Article 14, third paragraph, of the General Data Protection Regulation Implementation Act

(UAVG), the AP is authorized to impose an administrative fine with regard to infringements of the GDPR.

2.3.1 GDPR

Pursuant to Article 83, paragraph 1, of the GDPR, each supervisory authority ensures that the

administrative fines imposed under this Article for the offenses referred to in paragraphs 4, 5 and 6

reported infringements of this Regulation are effective, proportionate and dissuasive in each case.

Pursuant to paragraph 2, administrative fines shall be imposed, depending on the circumstances of the

specific case, imposed in addition to or instead of the provisions referred to in Article 58, paragraph 2, under a to h and under j,

referred measures.

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

It follows from the fourth paragraph, preamble and under a, that a breach of the obligation of the controller of Article 32 of the GDPR in accordance with paragraph 2 is subject to a administrative fine of up to €10,000,000 or, for a company, up to 2% of the total worldwide annual turnover in the previous financial year, if this figure is higher.

2.3.2 UAVG

Pursuant to Article 14, third paragraph, of the UAVG, the AP may, in the event of a violation of the provisions of Article 83, fourth, fifth or sixth paragraph, of the bye-law impose an administrative fine of at most the in amounts mentioned in these paragraphs.

3. Assessment

3.1 Processing of personal data

OLVG has been using a new and integrated hospital information system since October 19, 2015 electronic patient files are stored.2 The data about patients that OLVG has in the hospital information system is information that OLVG can use for natural persons identify. These patient data are therefore personal data within the meaning of Article 4(1) of the GDPR. Part of this data is health data and can therefore also be qualified as a special category of personal data within the meaning of Article 9 of the GDPR.

Furthermore, there is a processing of personal data within the meaning of Article 4, part 2, of the AVG. Due to its scope, the concept of "processing" includes any possible operation or set of processing of personal data. Capturing and viewing patient data in the hospital information system is also included. It concerns an extensive processing involving a lot people are involved. In 2018 alone, OLVG provided medical care to approximately 500,000 patients granted.3

3.2 Controller

In the context of the question of whether OLVG acts in violation of Article 32, first paragraph, of the GDPR, it is also important to determine who qualifies as a controller as referred to in Article 4(7), of the GDPR. It is decisive who has the purpose of and the means for the processing personal data - in this case the processing of patient data in the hospital information system of the OLVG - notes. In order to answer this question, the AP attaches importance to the statements from the board of OLVG during the on-site investigation, the registration in the trade register of the Chamber of Commerce, policy documents and the annual accounts of OLVG of 2015 and 2018.

2 On-site investigation dated May 22, 2019, Report 1: question 1.; Report 2: figures 2 to 7; Annual Report 2015 Stichting OLVG, p.16, 17;

Conversation report opinion session dated 25 June 2020, p. 6.

3 Annual Report 2018 OLVG, p. 5-6.

https://www.olvg.nl/sites/default/files/annual responsibility_2018_olvg_gewaarmerkt_dig_1.pdf

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

The chairman of the Board of Directors of OLVG has stated that in 2013 there will be an administrative merger took place between the Sint Lucas Andreas Hospital foundation and the Onze Lieve Vrouwen foundation Gasthuis and that there has been one joint board ever since.4 Then these two hospitals are in June Legally merged into one hospital in 2015, named: Stichting OLVG.5 Furthermore, during the merger in 2015, the current hospital information system has been uniformly introduced within OLVG.6 This system is like mentioned above, finally taken into use by OLVG on October 19, 2015.7

According to the registration in the Chamber of Commerce, OLVG's activities are 'general

hospitals, practices of medical specialists and medical day treatment centers, health centers and outpatient youth care."8 OLVG also mentions in its information security & privacy policy that the system of security and privacy measures focuses, among other things, on securing all information and information systems, preventing information security incidents and taking precautionary measures. The information security & privacy policy applies to all business units of the OLVG and on the exchange of data with other organisations.9 Also from the 'Regulation on patient data and use of means of communication' shows that OLVG has determined how OLVG employees have to deal with electronic patient files.10

Based on the above-mentioned documents and statements from the board of OLVG, the AP concludes that OLVG determines the purpose and means for the processing of personal data for the benefit of the OLVG electronic patient files. This means that OLVG is the controller in the meaning of Article 4, part 7, of the GDPR for the processing of patient data in the OLVG hospital information system.

3.3 Data Security Violation

3.3.1 Introduction

To ensure security and prevent the processing of personal data from being infringed to the GDPR, the controller must, pursuant to Article 32 of the GDPR, provide the assess inherent risks and take measures to mitigate risks. That measures must ensure an appropriate level of security, taking into account the state

4 On-site investigation dated May 22, 2019, Report 1: Board of Directors, question 1.

5 Annual Report 2015 OLVG, available at: https://www.olvg.nl/sites/default/files/jaarverresponsing_2015.pdf, p. 4, last consulted on: 30 July 2019. Also: on-site investigation dated 22 May 2019, Report 1: Board of Directors, question 1. OLVG also

two outpatient clinics in Amsterdam, see extract Chamber of Commerce: 41199082 under branches.

6 On-site investigation dated May 22, 2019, Report 1: Board of Directors, question 1; Annual Report 2015 OLVG, available via: https://www.olvg.nl/sites/default/files/annual responsibility_2015.pdf, p. 4, last accessed: 30 July 2019.

7 “In October 2015, the shared electronic health record (Epic) went live.”; Annual Report 2015 OLVG, available via: https://www.olvg.nl/sites/default/files/jaarverresponsing_2015.pdf, p. 17, last accessed: July 30, 2019; and article: https://www.medicalfacts.nl/2015/11/03/olvg-neem-elektronisch-patientendossier-epic-in-gebruik/. Conversation log opinion session dated 25 June 2020, p. 6.

8 OLVG East is the main location. Other branches are OLVG West, Jan Tooropstraat 164, 1061 AE in Amsterdam and the outpatient clinics
OLVG IJburg and OLVG Spuistraat. (excerpt from the trade register of the Chamber of Commerce of March 25, 2019.

9 OLVG response to AP information request dated 3 May 2019, Appendix 8.

10 OLVG response to AP information request dated 3 May 2019, appendix 28.

of the technique and the implementation costs compared to the risks and the nature of the protection personal data.11 In the following, the AP assesses whether OLVG has an appropriate level of security used for the processing of personal data in its hospital information system.

3.3.2 Two-factor authentication

3.3.2.1 Facts

The current hospital information system was taken into use by OLVG on 19 October 2015. During the day the on-site investigation on May 22, 2019 at OLVG, supervisors of the AP investigated how OLVG employees gain access to the electronic patient files (log in) within the hospital information system. The AP notes that the authentication of the identity of the employee to use the OLVG hospital information system in two ways depending on whether access is requested from inside or outside the OLVG network.

During the on-site investigation12, the AP supervisors established that employees

of OLVG on a computer (terminal) within the OLVG network can log in to the virtual workplace (VDI).13 Logging in is done by entering a user name and password and no use is made of a staff pass or a token as part of the login process to access the hospital information system. This way of logging in is different moments during the investigation on site. The regulators of the AP have this first observed during the demonstration of the hospital information system.14 This this observation is also confirmed by the oral statements of [CONFIDENTIAL].15

In addition, the AP supervisors during workplace inspections of three different employees16 of OLVG found that if the employee uses his/her user name and enters the password correctly, he/she will have access to the VDI environment and to the electronic patient records. It turned out that this involves a 'single sign on' functionality17, which means that the employee who is logged in to the VDI also has immediate access to the hospital information system with electronic patient records.

Furthermore, it is stated in Article 2.1. of the 'Regulation on patient data and use of means of communication' that “OLVG employees, (…) insofar as this is necessary for the position they perform within OLVG, by means of login code and password access [is] granted to the electronic patient record in Epic and similar patient information systems within OLVG (hereinafter collectively referred to as “EPD”).”18

11 Recital 83 of the GDPR.

12 On-site investigation dated 22 May 2019, Reports 2, 6, 7 and 8.

13 Virtual Desktop Infrastructure.

14 On-site investigation dated 22 May 2019, Report 2: questions 1 to 4 and figures 1 to 7. Demonstration by [CONFIDENTIAL] of OLVG.

15 On-site investigation dated 22 May 2019, Report 2: questions 1 and 2. And On-site investigation dated 22 May 2019, Report 2: questions 2 and 3.

16 Checking at the workplace of [CONFIDENTIAL] (Report 6), a [CONFIDENTIAL] (Report 7) and a [CONFIDENTIAL] (Report 8).

17 On-site investigation dated 22 May 2019, reports 7 and 8, not at the [CONFIDENTIAL] (report 6). See also the statement of [CONFIDENTIAL] of OLVG, on-site investigation dated 22 May 2019, Report 2: questions 2 and 3.

18 OLVG response to AP information request dated 3 May 2019, appendix 28. This document states that it is in force from 25 May 2018.

The second way to access the hospital information system is through a computer outside the OLVG network. During the demonstration during the on-site investigation, the AP observed that can also be logged into the VDI via a computer outside the OLVG network, for example when employees work from home.19 In this case, the VDI environment must be logged in and the hospital information system with a username and password20 in combination with a changing token that is received or created by SMS or application.21

On March 9, 2020, OLVG linked a reader to every computer (terminal) and thus the above method changed. As a result, an employee must present his/her personnel pass for this reader and then enter a password before accessing the computer obtained.22

3.3.2.2 Assessment

Pursuant to Article 32, paragraph 1, of the GDPR, the controller must take appropriate steps take technical and organizational measures to ensure a level of security appropriate to the risk to ensure. According to Article 32, second paragraph, of the GDPR, attention should be paid to the assessment of the risks to be spent on risks that arise in the processing of personal data. As the data is of a more sensitive nature, or the context in which it is used poses a greater threat forms for the privacy of those involved, stricter requirements are imposed on the

data security.

OLVG processes personal data of approximately 500,000 patients in its hospital system on a large scale.

This (often) involves extremely sensitive health data. Health data is out

designated as a special category of personal data pursuant to Article 9(1) of the GDPR.

These personal data which, by their nature, are particularly sensitive in terms of fundamental rights and

fundamental freedoms, deserve specific protection given the context of their processing

can pose significant risks to fundamental rights and freedoms. OLVG serves

therefore take appropriate measures to protect personal data as well as possible and

infringements as much as possible.

Given the sensitive nature of the data, the large scope of the processing by OLVG and the risks

OLVG had regard to the privacy of data subjects when accessing personal data

electronic patient records must implement two-factor authentication. The AP has in it

However, it has been established above that employees can access a computer within the OLVG network

could get to the data in electronic patient records with just something an employee

know (namely a username and password). That means that in that case it was used

of only one factor. The investigation has shown that OLVG did not make use of

a pass, token or other second factor. This means that OLVG does not meet the minimum requirement

19 On-site investigation dated May 22, 2019, Report 2: authentication, question 4.

20 On-site investigation dated 22 May 2019, Report 2: figure 7 portal.olvg.nl.

21 On-Site Survey dated May 22, 2019, Report 2: Authentication, Question 4, Figure 7-13.

22 Written opinion OLVG, 27 March 2020, p. 24 and 25. OLVG oral opinion, 25 June 2020, p. 4.

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

two-factor authentication fulfilled, which in the context of this processing under Article 32 of the AVG is required. The AP considers such a security measure, also given the current state of the technique and implementation costs, appropriate. In doing so, the AP takes into account that general accepted security standards, such as the Dutch standard for information security in healthcare, prescribe two-factor authentication.

OLVG has further indicated in its Information Security & Privacy Policy that the aforementioned policy is based on: 1) the Dutch standard for information security in healthcare, namely: NEN 7510, NEN 7512 and NEN 7513 and 2) the current laws and regulations, including the AVG. OLVG strives for it to demonstrably comply with these standards.23 OLVG has therefore also independently committed itself to comply with the above NEN standards, which stipulate that the identity of users must are established by means of two-factor authentication.24

Needless to say, the AP finally notes that specifically with regard to the wording 'appropriate technical and organizational measures' - as included in article 32 AVG - there is a continuation of what already applied under Directive 95/46/EC and the Personal Data Protection Act (Wbp).25 There is no material change. Under those circumstances, it's obvious — also with a view to legal certainty — to continue the interpretation followed in the past in the interpretation of Article 32, first paragraph, of the GDPR. This means that the interpretation already used in the past via the requirements of two-factor authentication contained in the NEN standards and the regular assessment of the log files are maintained.26 The AP has also always clearly communicated that the NEN 7510, as generally accepted security standard within the practice of information security in healthcare, remains an important standard for information security in healthcare under the AVG regime and this one guidelines must be followed.27

Opinion OLVG and response AP

OLVG states in its view that the AP wrongly judges that OLVG does not use two-factor authentication has applied. According to Norm 9.4.1 of NEN 7510-2 (2017), health information systems that process personal health information, identify users and this should be done

to be done through authentication involving at least two factors.

According to OLVG, access to PCs has been limited for years by access to the physical space

where the PC is. PCs are in rooms that can only be accessed with a

personal personnel card. The pass is configured in such a way that an employee can only

23 OLVG response to AP information request dated 3 May 2019, Appendix 2, under 3.3 and Appendix 8 under 2.2.

24 Incidentally, healthcare providers are, pursuant to Articles 3 and 5 of the Electronic Data Processing by Healthcare

Providers Decree

obliged to ensure the safe and careful use of electronic equipment in accordance with NEN 7510 and NEN 7512.

exchange systems and that logging complies with the provisions of NEN 7513.

25 Article 13 Wbp and Article 17(1) of Directive 95/46/EC already used the terminology 'appropriate and organizational

measures'

to prevent loss or unlawful processing.

26 For example, it follows from the report 'access to digital patient files within healthcare institutions' of June 2013;

https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-patientendossiers-binnen-

healthcare institutions.pdf.

27 Cf.: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorgproviders-en-de-avg; See also communication

by AVG

helpdesk Care at https://www.avghelpdeskzorg.nl/onderwerpen/veiligheid/nen-7510.

has access to areas and functions for which the employee is authorized. According to OLVG, there is none

difference in principle between access that is limited to the person who holds a pass in front of a reader who is

located at the PC.

The AP does not follow OLVG's view. For appropriate security of personal data
electronic patient files, it is necessary that the OLVG information system only contains a
two-factor authentication is accessible. If access to the room is charged with an authentication via
a personal pass but the computer itself not with a two-factor authentication, then the chances are greater
employees who are authorized for the room (such as cleaners) but not for the electronic
patient records, can access these records. In addition, certain parts of the
hospital, such as outpatient clinics, are not completely closed. So there is indeed an important difference with the
access restricted to the person holding a pass in front of a reader located at the computer.
Finally, the AP emphasizes that standard 9.4.1 of NEN 7510-2 (2017) uses the term 'health information systems'
contains. In other words, the information systems themselves must be secured with two-factor authentication.
In view of the foregoing, the DPA is of the opinion that OLVG will in any event until 22 May 2019 apply article 32, first
paragraph,
of the GDPR, now that OLVG's hospital information system has not complied with it
requirement of two-factor authentication. OLVG has now terminated this violation by informing each
computer (terminal) to connect a reader. As a result, an employee must present his/her personnel card
in front of this reader and then enter a password before accessing the computer
be obtained.

3.3.3 Logging check

3.3.3.1 Facts

OLVG's Information Security & Privacy Policy states that OLVG is committed to it
demonstrable compliance with the standards NEN 7510 (information security in healthcare), NEN 7512
(based on trust for data exchange), NEN 7513 (logging actions on electronic
patient files) and the AVG.28 Moreover, OLVG indicates in the Logging policy Epic that this document
must lead to compliance with the NEN 7513 standard and applicable laws and regulations.29 In the Logging
Epic's policy is based on the principle that the log files are periodically checked for
indications of irregularities or errors so that they can be detected early where necessary

overcome.30 To this end, all activities of users, systems and

information security events recorded in log files.31 Of anomalous events

registered in the log data, a report is drawn up and, if necessary, further action is taken

research.32 The Logging policy Epic makes a distinction in the way in which the log data

are checked, namely on a random basis and on an incident basis.33

28 Study of 10 February 2020, Annex 2, under 3.3 and Annex 8 under 2.2.

29 Study of 10 February 2020, appendix 13, under 2.1.

30 Study of 10 February 2020, appendix 13, under 4.4.

31 Study of 10 February 2020, appendix 13, under 4.2.

32 Study of 10 February 2020, appendix 13, under 4.7.

33 Study of 10 February 2020, appendix 13, under 4.6.

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

Based on Epic's Logging Policy, random checks must be carried out every four weeks

representative sample must be taken for analysis.34 The Logging procedure Epic shows this

a monthly report is obtained from the data warehouse of the number of break-the-glass

events.35 There will always be an average number of events.36 The EPD Service does random checks

control of the break-the-glass events and is free to determine what constitutes a representative one

sample.37 If there are major deviations for one or more users, further investigation is required

investigation into these deviations.38 The incidental check takes place when the

current events (from an incident or a request from a patient) give rise to this.39 Then the

necessary analyzes are performed. In this case, if there is a request from a patient,

the research question must come from Legal Affairs.40 Of anomalous events

reports are drawn up.41 The report shows what the notable events are

are and how or why these events stand out, and how they conflict with policy

and/or lawful access to a file.42

[CONFIDENTIAL] of OLVG stated during the on-site investigation that every action is

logged.43 [CONFIDENTIAL] of OLVG has stated that with regard to checking the logging

a number of random checks and incidental checks have been carried out.44 For example, on 26 March 2018 a random check

done to the break-the-glass behavior of certain job groups.45 This pertained to the job groups

nurses and doctors in training and covered a period of three months.46 The report that

has been drawn up as a result of this sample consists of one page of figures and a graph of it

total number of break-the-glass per month, without analysis of the aforementioned figures.47

On March 13, 2019, a report was also drawn up containing the analysis of the sample by break-

the-glass use by working students.48 The report of the analysis consists of eight pages with a

numerical overview and analysis of deviating break-the-glass use in the period from January 1, 2018 to

and with 7 February 2019 of all 181 working students who were still employed by OLVG on 6 February 2019.49

34 Study of 10 February 2020, appendix 13, under 4.6.

35 Study of 10 February 2020, appendix 14, under 3.4.

36 Study of 10 February 2020, appendix 14, under 3.4.

37 Study of 10 February 2020, appendix 14, under 3.4.

38 Study of 10 February 2020, appendix 14, under 3.4.

39 Study of 10 February 2020, appendix 13, under 4.6.

40 Study of 10 February 2020, appendix 13, under 4.6.

41 Study of 10 February 2020, appendix 14, under 3.5.

42 Study of 10 February 2020, appendix 14, under 3.5.

43 On-site investigation of 22 May 2019, interview report 4, under 1.

44 On-site investigation of 22 May 2019, interview report 4, under 5.

45 On-site investigation of 22 May 2019, interview report 4, under 5.

46 On-site investigation of 22 May 2019, interview report 4, under 7.

47 Study of 10 February 2020, appendix 25.

48 On-site investigation of 22 May 2019, interview report 4, under 5 and Investigation of 10 February 2020, appendix 24.

49 Study of 10 February 2020, appendix 24.

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

[CONFIDENTIAL] of OLVG has stated that these two samples are the only two samples
have been carried out by OLVG in the period from 1 January 2018 to 22 May 2019.50
In addition, [CONFIDENTIAL] of OLVG has stated that OLVG believes that a collection
of incidental checks also forms a sample, since it is examined in an aggregated manner
it often happens that there has been unauthorized access and what incidents this concerns.51 According to the
[CONFIDENTIAL] of OLVG, very few irregularities were found and formed
not a specific reason to schedule another sampling.52 [CONFIDENTIAL] stated that
there is not, as described in the logging policy, a random check every four weeks
takes place, but that in practice one looks at what gives rise to doing a
sample.53 The samples mentioned above are the only two samples that have been carried out.54 At the time
of the on-site investigation, an alarm at certain limit values was still being developed.55
In addition to these two random checks, OLVG also carried out incidental checks. OLVG has in the period
eight incident checks were carried out from January 2018 to April 2019.56 This concerns the requesting of
one electronic patient record at a time in response to a patient request.57
Following the opinion hearing of 25 June 2020, OLVG issued additional information on 13 July 2020
written documents, including a data query on all logging data, reports of
samples from different perspectives and reports resulting from the newly applied

selection method.

3.3.3.2 Assessment

It has already been explained in paragraph 3.3.2.2 that the controller under Article 32,

paragraph 1 of the GDPR must take appropriate technical and organizational measures to ensure that the

risk-appropriate level of security.

The AP has determined that in the period from January 1, 2018 to April 17, 2019, OLVG, two broader

performed (sample) checks of break-the-glass behavior over larger groups of employees

and eight incidental checks of the logging of one electronic patient record. Furthermore, the AP

determined that in the period from 1 January 2018 to 22 May 2019 OLVG did not systematically

checks for notable deviations from all logging of all electronic health records

performed, nor applied systematic or automatic signaling when exceeding

certain limits in the logging involving all logging of all electronic health records

has been involved.

50 On-site investigation of 22 May 2019, interview report 4, under 5, 10 and 16.

51 On-site investigation of 22 May 2019, interview report 4, under 8.

52 On-site investigation of 22 May 2019, interview report 4, under 8.

53 On-site investigation of 22 May 2019, interview report 4, under 16.

54 On-site investigation of 22 May 2019, interview report 4, under 16.

55 On-site investigation of 22 May 2019, interview report 4, under 17.

56 Study of 10 February 2020, appendices 16 to 23.

57 Study of 10 February 2020, appendices 16 to 23.

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

In its opinion, OLVG indicates that the protocol "procedure for checking the legality of file inspection" has been updated and re-established on March 17, 2020. Since the on-site investigation of the AP in May 2019 further tightened. As of July 1, 2019, OLVG has the frequency of checking the logging has already been increased to once every two weeks (at least two or more reports per month). This check includes a (biweekly) data query on all logging data.
In the period from July 2019 to November 2019 there are reports based on logging data made from different perspectives. From these different perspectives is in this period reported several times about the logging behavior. The different perspectives have also been used to determine where the risk of unauthorized access is greatest. It started in May 2020 with a new selection method. All contacts are assigned a score with a higher score means more chance of unauthorized access. As of June 2020, at least every two weeks made a printout of 50 views with the highest point score on a random day, which was assessed and subsequently further investigated if there is a suspicion of unlawfulness. In addition to the random check, an ad hoc logging check takes place if the topicality (from solving of incidents or from a patient's request) gives rise to this. OLVG believes that this complies with standard 12.4.1 of NEN 7510-2 (2017).
As mentioned above, the DPA has established that in the period from 1 January 2018 to 17 April 2019, two spot checks and eight incidental checks of the logging of one electronic patient file. OLVG therefore has at least during the aforementioned period not in accordance with its own policies (including the Information Security & Privacy Policy and Logging Policy Epic) acted. Aside from that, it's only doing eight incidental checks and two proactive ones samples in a period of 15.5 months amply and clearly insufficient to be able to speak of an appropriate security level that pertains to signaling unauthorized access to patient data and taking measures in response to unauthorized access. In doing so, the AP matters the scale of the hospital's processing of health data, the sensitive nature of the data and the risks to the privacy of those involved.

OLVG processes (special categories of) personal data on a large scale and (mostly) this involves highly sensitive health data. Therefore, stricter requirements are imposed on the security of this data. Given the sensitive nature of the data, the large size of the processing and the risks to the privacy of those involved, OLVG therefore had the check log data regularly. In this way, unauthorized access can be signaled and take action. The starting point of the AP is that monitoring of the logging is systematic and must take place consistently, with a random check and/or check based on complaints is not enough. 58 The fine-meshed nature of the authorization model used and the control of the the correctness of the authorizations partly determines the intensity of the monitoring of the logging. At one random random checks, there is no question of a system aimed at unlawful use and risks. As a result, OLVG does not meet the requirement of regular assessments log files are met, which is in the context of this processing under Article 32 of the GDPR required. The AP considers such a control measure, also in view of the current state of the art and the

58 See also the report “Access to digital patient records within healthcare institutions” of June 2013.

implementation costs, appropriate. In doing so, the AP takes into account that generally accepted security standards, such as the Dutch standard for information security in healthcare, on a regular basis prescribe logging.

Finally, as in section 3.3.2.2. already appointed, also independently committed to comply with NEN standards. Section 12.4.1 of NEN 7510-2 states that log files of events that include user activities, exceptions, and information security events record, should be made, kept and regularly reviewed.

In view of the foregoing, the DPA is of the opinion that OLVG will in any event until 22 May 2019 apply article 32, first paragraph,
of the GDPR because OLVG has not regularly reviewed log files. OLVG has
meanwhile this violation has been terminated by the procedure with regard to the control of the logging
tightened and increased the frequency of checking the logging.

3.4 Other view OLVG and response AP

3.4.1 Rights of the Defense

OLVG argues that the imposition of a fine for the conduct established by the AP is in violation of
the nemo-tenetur principle59 as laid down in Article 48(1) of the European Charter and Article
6, paragraph 1, of the European Convention on Human Rights (ECHR), since the
findings are based on data breach reports that OLVG was obliged to make under threat
of a sanction. Referring to various case law, OLVG states that if during a
procedure there is (the reasonable expectation) of a criminal charge, at least when this is not possible
It is excluded that the material will also be related to a criminal charge against the provider
used, the nemo-tenetur principle precludes it from being obtained in the procedure
volitional material is used for an administrative punishment through
fine.60

The fact that OLVG, pursuant to the Electronic Data Processing by Healthcare Providers Decree and the
NEN standards contained therein, it is required to keep certain log files which allow the supervision of the
makes compliance with the GDPR possible, does not mean that there is independence of will, according to OLVG
evidence. Pursuant to article 33, first paragraph, of the GDPR, OLVG has on September 13, 2018 and on
February 15, 2019, a report of a data breach was submitted to the AP. These data breach reports concern according to
OLVG information that does not exist apart from the will of OLVG: OLVG has compiled the information to
comply with the obligation of Article 33, first paragraph, of the GDPR. Referring again to several
court rulings, OLVG argues that voluntary information may not be used for a
administrative punishment by means of a fine.61 In response to the two

data breach reports initiated an investigation in the context of which the investigation took place on May 22, 2019

59 The principle that no one is bound to testify against himself or make a confession.

60 Conclusion A-G Vegter 16 May 2018, ECLI:NL:PHR:2018:441, r.o. 4; CBb 7 May 2019, ECLI:NL:CBB:2019:177, r.o. 5.3.2; Supreme Court July 12, 2013,

ECLI:NL:HR:2013:BZ3640;

61 Supreme Court 12 July 2013, ECLI:NL:HR:2013:BZ3640, r.o. 3.8 and 3.9.; HR 24 April 2015, ECLI:NL:HR:2015:1117, ECLI:NL:HR2015:1129,

ECLI:NL:HR:2015:1130, ECLI:NL:HR2015:1137 and ECLI:NL:HR:2015:1141; CBb 7 May 2019, ECLI:NL:CBB:2019:177, r.o. 5.3.8 and 5.3.10.

occurred. According to OLVG, it is therefore clear that the entire investigation of the AP is based to the notifications made by OLVG on the basis of the GDPR.

In a letter dated 17 April 2019, the AP furthermore, pursuant to Sections 5:16 and 5:17 of the General Act administrative law (Awb) requested information. In this letter, the AP did not point out that OLVG does not is obliged to provide information if this would prove a violation of the GDPR to deliver. According to OLVG, this means that all information that the AP has obtained with its request for information, was obtained under duress as referred to in Article 6, paragraph 1, ECHR and Article 48, paragraph 1 member of the Charter. OLVG concludes that, in view of the foregoing, voluntary information that obtained under duress from OLVG cannot be used for imposing an administrative sanction fine.

Reply AP

The AP does not follow OLVG's view. The AP is of the opinion that the evidence it has obtained is not in

contrary to Article 48, first paragraph, of the European Charter and Article 6, first paragraph, ECHR and the closed nemo-tenetur principle is obtained. Nor should evidence be excluded. AP motivates that as follows.

First of all, the AP will address the two data breach reports. As OLVG itself indicates, the two are reported data leaks have only been a reason for the AP to start an official investigation into the compliance with Article 32 of the GDPR by OLVG. The two data breach reports are in the file with the documents relating to the case, but they do not constitute evidence in any way of the violation of Article 32 of the AVG found by the AP. exclusion of those data breach reports as evidence is therefore not an issue. Separately, the AP considers the data breach notification as independent information. In view of Article 33 paragraph 5 of the AVG, OLVG is obliged all personal data breaches, including the facts surrounding the breach in connection with personal data, the consequences thereof and the corrective measures taken document, so that it is deemed to have had this information.62

Secondly, the DPA does not follow OLVG in its statement that the DPA with its information request of 17 April 2019 OLVG has forced it to provide information to the AP and therefore not to use that information may be subject to an administrative fine. It is first of all relevant to determine this that the AP requested information in that letter. There is no formal information 'advanced' under it reference to the obligation to cooperate, as follows, for example, from Article 5:20 of the Awb and/or Article 31 of the GDPR. That the relevant letter refers to article 58, first paragraph under a, GDPR and article 5:16 yo. 5:17 Awb doesn't change this. These references are for information purposes only for OLVG included the letter in order to make it clear that the AP (and its employees) OLVG to that may request information and on what basis they may do so. From providing information under In the opinion of the AP there is therefore no question of coercion.

In addition, if and insofar as exclusion of evidence would (yet) be at issue, such exclusion according to settled case law applies only to evidence the existence of which depends on the will of the person

62 See also ABRvS 8 April 2020, ECLI:NL:RVS:2020:1011, l.o. 2.2.

provider (will dependent material). This does not apply to evidence that exists independently of the will of the provider (independent material). The AP has from OLVG in response to it information request from the AP dated May 3, 2019 both voluntary material (statements and explanations prepared for the AP) as independent material. It

Independent material consists of documents that already existed in a physical sense at OLVG, such as the logging policy dated 29 September 2016 and reports of samples dated 13 March 2019 resp. March 26 2018. The AP subsequently did not use the voluntary material to determine the violation and the imposition of an administrative fine. The violation is, however, independent of will material, partly based on volitional material that was later provided by OLVG employees after they have been made aware of the right to remain silent by means of the caution. Evidence exclusion is at the discretion of the AP is therefore not relevant for that reason.

On the basis of the above, the AP concludes that a fine should be imposed for the identified conduct is not in conflict with the nemo-tenetur principle as laid down in Article 48(1) of the European Charter and Article 6, paragraph 1, ECHR.

3.4.2 Research purpose

OLVG argues that the imposition of a fine for the conduct, at least with regard to authentication, is contrary to the rights of the defence as laid down in Article 48(2) of the European Charter and Article 6(2) ECHR, since the established behaviors fall outside the scope of the AP previously formulated research goal.

According to OLVG, the AP does not conclude in the investigation report that OLVG is not suitable

has taken technical and organizational measures to ensure that personal data
in the electronic patient record are not consulted by unauthorized employees. But the
AP finds that OLVG does not meet the requirement of at least two-factor authentication pursuant to
Article 32, first paragraph, opening words, of the GDPR. Prevents a two-factor authentication as the AP fills it in
according to OLVG, the behavior of the employees involved is not. With a two-factor authentication
all employees, including the working students, have a pass, token, or another second factor.
Having them does not mean that they would not be able to perform the behaviors to which the
saw data breach notifications. These employees would also use a two-factor authentication such as the AP
fills in have had the authorization they currently have.

Reply AP

The AP does not follow OLVG's view. The AP has informed OLVG that the AP is investigating
whether OLVG's technical and organizational measures are 'appropriate' as referred to in Article 32 of the
AVG, in order to ensure that personal data in the electronic health record is not
consulted by unauthorized personnel. The AP has explicitly mentioned that the investigation
focuses on logical access security (authentication and authorization), logging, control of the
logging and employee awareness.

The AP's conclusion that OLVG does not comply with Article 32, first paragraph, of the GDPR, now that the
the requirement of two-factor authentication is directly related to the research objective and falls within the
scope of the research objective. After all, the AP mentions Article 32, first paragraph, of the GDPR, as the
associated guarantee and explicitly the logical access security (authentication and authorization) in it
research purpose. In the context of the right of defense it is irrelevant whether employees of OLVG

with or without two-factor authentication would have had the same authorization in practice.

The AP notes unnecessarily that in its research objective it recognizes the fact that personal data in the electronic health records should not be accessed by unauthorized employees warranty mentioned. To minimize the risk of unauthorized access to patient data It is very important to establish the correct identity of the employee in advance. That two factor authentication is not a measure that guarantees that unauthorized access to patient records by employees no longer occurs, does not alter the fact that it is a measure that is important contributes to the prevention of unauthorized access and in this case is required under Article 32 of the GDPR. In this context, the AP emphasizes that applying two-factor authentication and also control on the logging does not stand alone, but should be viewed in conjunction with all others appropriate measures. It is the combination of these measures that enables OLVG to to manage the protection of personal data as well as possible and to prevent infringements as much as possible prevent. Applying a two-factor authentication does not release OLVG from the obligation to promote awareness among employees about patient privacy protection.

3.4.3 Implementation of Article 32 of the GDPR

OLVG takes the position that the GDPR does not allow member states and therefore the national legislator any scope offers to further detail the assessment against the standard of Article 32 of the GDPR by means of NEN-standards. According to OLVG, the AP therefore acts in violation of the GDPR because of that in the research report do. OLVG argues that Member States can only go further than the regulation given protection, and may only further specify this protection if this is explicitly stated in the GDPR has been determined. According to OLVG, this is not the case. According to OLVG, the trade-offs between a number of aspects as included in article 32 of the AVG not made by the AP, which is in conflict with the due diligence principle. Finally, in the opinion of OLVG, the NEN standards cannot be used as a basis form for the interpretation of Article 32 of the GDPR, now that these standards are not mentioned by the GDPR and have been created without being related to or based on the GDPR.

Reply AP

The AP does not follow OLVG's view in this either. OLVG refers to the prohibition on further (binding)
to set rules in national regulations in case a European regulation applies and this one
regulation does not explicitly allow this. However, such a situation does not arise in the present case. To the
In the opinion of the AP, Article 6, paragraphs 2 and 3, of the GDPR expressly offers the right to do so
possibility. This does not alter the fact that Article 32 of the GDPR has been applied in the specific case and
interpreted. The application and interpretation is - in view of the hair in Article 6, third paragraph, of the UAVG
task assigned to monitor compliance with the GDPR - to the AP. That is what the AP
has done in the research report and what it is obliged to do.

In answering the question of whether there are appropriate technical and organizational measures in place
of Article 32 of the GDPR, it is relevant what is included in the relevant NEN standards. This
after all, standards are generally accepted security standards within the practice of the
information security in healthcare. The requirement of two-factor authentication contained in these NEN standards and the
obligation to regularly assess the log files, the AP considers a concrete interpretation of what if
'appropriate' can be considered within the meaning of Article 32 of the GDPR. That the NEN standards are not in the GDPR
are mentioned and have been established without being related to or based on the GDPR
the AP deems irrelevant. After all, Article 32 of the GDPR provides a standard that is aimed at all
controllers in all segments of the market. Referring to sections 3.3.2 and 3.3.3
the DPA has assessed whether OLVG has taken sufficient appropriate security measures such as
referred to in Article 32 of the GDPR, 'deducted taking into account the state of the art and the implementation costs
against the risks and the nature of the personal data to be protected". The AP has the presence in that consideration
of generally accepted security standards such as the NEN standards

taken and allowed to take.

Moreover, OLVG itself has also indicated that in its Information Security & Privacy Policy

the aforementioned policy is based on the Dutch standard for information security in healthcare, namely:

NEN 7510, NEN 7512 and NEN 7513 and current legislation and regulations, including the GDPR.63 In its

Logging policy Epic indicates to OLVG that this document must lead to compliance with NEN7513 and

applicable laws and regulations.64 In short, the AP deduces from this that OLVG is also of the opinion that these

NEN standards give substance to the correct degree of information security and therefore act independently

has committed to comply with the above NEN standards.

3.4.4 Decree on electronic data processing by healthcare providers

The AP's investigation report refers to Article 3(2) of the Decree

electronic data processing by healthcare providers (Begz). It states that a

care provider, in accordance with the provisions of NEN 7510 and NEN 7512, ensures a safe and

careful use of the healthcare information system and safe and careful use of the electronic system

exchange system to which it is connected. OLVG states that the AP only imposes a fine or burden

can impose a penalty to enforce the obligations imposed in the GDPR and not for a

violation of the Begz. The Begz has been established on the basis of Article 26 of the Wbp and not on the basis of the

UAVG. Pursuant to Article 51 UAVG, the Wbp lapsed on 25 May 2018. That is also the basis

of the Begz with effect from that date.

Reply AP

Finally, the AP does not follow OLVG's view in this regard either. As will be in the next chapter

explained, the AP has imposed an administrative fine for the violation of Article 32, paragraph 1 of

the GDPR, more specifically with regard to authentication and regular checking of the log files.

Incidentally, the Begz does apply to the OLVG and the standards are mandatory on the basis of the Begz

NEN 7510 and NEN 7512.

63 Study of 10 February 2020, Annex 2, under 3.3 and Annex 8 under 2.2.

64 Study of 10 February 2020, appendix 13, under 2.1.

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

4. Fine

4.1 Introduction

From May 25, 2018 to at least May 22, 2019, OLVG violated Article 32, first paragraph, of the GDPR by not meeting the requirement of two-factor authentication and regularly reviewing log files.

The AP uses its authority to impose a fine on OLVG for the established violation to be imposed on the basis of Article 58, second paragraph, opening lines and under i and Article 83, fourth paragraph, of the GDPR, read in conjunction with Article 14, third paragraph, of the UAVG. The AP uses the Fining Policy Rules 2019.65

After this, the AP will first briefly explain the fine system, followed by the reasons for the fine fine in this case.

4.2 Penalty Policy Rules of the Dutch Data Protection Authority 2019

Pursuant to Article 58, second paragraph, opening words and under i and Article 83, fourth paragraph, of the GDPR, read in connection with Article 14, third paragraph, of the UAVG, the AP is authorized to inform OLVG in the event of a to impose an administrative fine of up to € 10,000,000 in violation of article 32, first paragraph, of the AVG or, for a company, up to 2% of the total worldwide annual turnover in the previous financial year, if this figure is higher.

The AP has established Fining Policy Rules regarding the implementation of the aforementioned power to imposing an administrative fine, including determining the amount thereof.

Pursuant to Article 2, under 2.1, of the Fining Policy Rules, the provisions regarding violation

of which the AP can impose an administrative fine not exceeding € 10,000,000 (or for

a company up to 2% of the total worldwide annual turnover in the previous financial year, if this figure

is higher) classified in Annex 1 as Category I, Category II or Category III.

In Annex 1, Article 32 of the GDPR is classified in category II.

Pursuant to Article 2, under 2.3, the AP sets the basic fine for violations for which a legal

maximum fine of € 10,000,000 or, for a company, up to 2% of the total worldwide

annual turnover in the previous financial year, if this figure is higher, [...] fixed within the next

fine bandwidth:

Category II: Fine range between €120,000 and €500,000 and a basic fine of €310,000. […].

65 Stct. 2019, 14586, March 14, 2019.

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

Pursuant to Article 6, the AP determines the amount of the fine by increasing the amount of the basic fine (to

at most the maximum of the bandwidth of the fine category linked to a violation) or

down (to at least the minimum of that bandwidth).

Pursuant to Article 7, without prejudice to Articles 3:4 and 5:46 Awb, the AP takes into account the factors that

are derived from article 83, second paragraph, of the AVG and in the Policy Rules referred to under a to k.

4.3 Fine amount

4.3.1. Nature, seriousness and duration of the infringement

Pursuant to Article 7, preamble and under a, of the Fining Policy Rules 2019, the AP takes into account the nature,

the seriousness and duration of the infringement. In assessing this, the AP takes into account, among other things, the nature,

the

scope or purpose of the processing as well as the number of data subjects affected and the scope of the processing

damage suffered to them.

Any processing of personal data must be done properly and lawfully. Personal data

must be processed in a manner that ensures appropriate security and confidentiality of that

guarantees data. Also to prevent unauthorized access to or use of

personal data and the equipment used for the processing. The

The controller must therefore provide appropriate and

take technical and organizational measures to ensure a level of security appropriate to the risk

to ensure. In determining the risk for the data subject, the nature of the

personal data and the nature of the processing are important: these factors determine the potential damage

for the individual data subject in the event of, for example, loss, alteration or unlawful processing of the

facts. The AP has come to the conclusion that OLVG has not applied an appropriate security level

for the processing of personal data in its hospital information system.

The AP has determined that OLVG will process personal data without appropriate data until at least 22 May 2019

processed security. This personal data contains highly sensitive patient information

OLVG, such as a wide variety of health data. It is important that OLVG

processes personal data of hundreds of thousands of patients. This large group of stakeholders has

unnecessary additional risk of, among other things, unauthorized access to their personal data. The fact that

the violation has continued in a structural manner for a longer period, also under the Wbp

under which an appropriate security level was already required, the AP considers serious. That it is also one

processing of particularly sensitive data makes insufficient security of the

personal data extra blame.

In view of the nature, seriousness, scope and duration of the infringement, the DPA sees reason to set the basic amount

of the fine pursuant to Article 7, preamble and under a, of the Fining Policy Rules to be increased by

€80,000 to €390,000.

4.3.2 Culpability and negligent nature of the breach

Pursuant to Section 5:46(2) of the Awb, when imposing an administrative fine, the AP

take into account the extent to which this can be attributed to the offender. Now that this is one

violation, it is not required for the imposition of an administrative fine in accordance with established case law
it is demonstrated that there is intent and the AP may assume culpability if the
perpetrator is established. In addition, the AP, pursuant to Article 7, under b, of the Fining Policy Rules
2019 take into account the willful or negligent nature of the breach.

OLVG is required by Article 32 of the GDPR to implement security measures that
are appropriate for the nature and scope of the processing operations that OLVG carries out. Now OLVG for longer
period no two-factor authentication and regularly checking the log files in her
organization has implemented, the AP is of the opinion that OLVG is in any case particularly negligent
in not taking such measures. Partly in view of the sensitive nature, OLVG is allowed
the large volume of processing, however, it is expected that it adheres to the applicable standards
ascertained and acted accordingly. The AP considers this culpable.

In addition, OLVG has indicated the aforementioned in its own Information Security & Privacy Policy
policy is based on the Dutch standard for information security in healthcare, namely: NEN 7510,
NEN 7512 and NEN 7513 and current laws and regulations, including the GDPR. OLVG strives for this
demonstrable compliance with these standards. OLVG has also stipulated in its logging policy that it is responsible for the
control of the log data takes a representative sample to analyze every four weeks. It
The fact that OLVG therefore also does not comply with its own existing policy rules is considered very negligent by the AP. It
had
on the way of OLVG to implement the standards and the violation of Article 32 of the
AVG as soon as possible, so that, among other things, to signal unauthorized access to

patient data and taking measures in response to unauthorized access is guaranteed.

In view of the negligent nature of the infringement, the AP sees reason to base the basic amount of the fine of article 7, under b, of the Fining Policy Rules 2019 to be increased by €50,000 to €440,000.

4.3.3 Proportionality

Finally, pursuant to Articles 3:4 and 5:46 of the Awb, the AP assesses whether the application of its policy for determining the amount of the fine in view of the circumstances of the specific case, not one disproportionate outcome. The AP is of the opinion that, given the seriousness of the violation and the extent in which this can be blamed on OLVG, the (amount of) the fine is proportionate.66 The AP sees no cause the amount of the fine on the basis of proportionality and the other in Article 7 of the Penalty Policy Rules mentioned circumstances, insofar as applicable in the present case, te increase or decrease.

4.4 Conclusion

The AP sets the total fine amount at €440,000.

66 See sections 4.3.1 and 4.3.2.

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

5. Operative part

fine

The AP imposes an administrative fine on OLVG for violation of Article 32, first paragraph, of the AVG amounting to € 440,000 (in words, four hundred and forty thousand euros).67

Yours faithfully,

Authority for Personal Data,

e.g.

drs. C.E. Mur

Board member

Remedies Clause

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

decides to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority. Submit it

of a notice of objection suspends the operation of this decision. For submitting a digital objection, see

www.autoriteitpersoonsgegevens.nl, under the heading Objecting to a decision, at the bottom of the

page under the heading Contact with the Dutch Data Protection Authority. The address for submission on paper

is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague.

Mention 'Awb objection' on the envelope and put 'bezwaarschrift' in the title of your letter.

Write in your notice of objection at least:

- your name and address;

- the date of your objection;

- the reference referred to in this letter (case number); or enclose a copy of this decision;

- the reason(s) why you disagree with this decision;

- your signature.

67 The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (CJIB).