Confidential/Registered

OLVG . Foundation

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

Chairman of the Board

PO Box 95500

1090 HM Amsterdam

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Topic

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

authority 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 on a regular basis. As a result, OLVG has insufficiently appropriate

measures taken as referred to in Article 32, first paragraph, 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 responsibility for processing and the violation. Chapter 4 sets out the (level of the) administrative fine 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 with 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 functions.1

The AP has received two data breach notifications 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 OLVG's compliance with Article 32(1) of the GDPR by to examine security aspects such as the authentication and control of the logging, among other things.

1.2 Process

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

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

The AP sent the report with findings to OLVG on February 10, 2020. By letter of 17 February

In 2020, the AP sent OLVG an intention to enforce. To this end also with this letter by

given the AP the opportunity, OLVG wrote to OLVG on 27 March 2020 and orally on 25 June 2020

gave its opinion on this intention and the report on which it is based.

2. Legal framework

2.1 Scope GDPR

Pursuant to Article 2(1) of the GDPR, this Regulation applies to all or part of

automated processing, as well as to the processing of personal data that are in a file

included or intended to be included therein.

Pursuant to Article 3(1) of the GDPR, this Regulation applies to the processing of

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

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

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 is carried out 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 about 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” means a […] legal entity that, alone or jointly with others, fulfills the purpose of

and determine 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(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

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

freedoms of persons, appropriate technical and organizational measures to

ensure an appropriate level of security […].

Pursuant to the second paragraph, in the assessment of the appropriate security level, particular account shall be taken of:

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

unauthorized disclosure or access to transmitted, stored or otherwise

processed data, either accidentally or unlawfully.

2.3 Administrative fine

Pursuant to Article 58, second paragraph, preamble and under i, in conjunction with Article 83, fourth paragraph, preamble and

under

a, of the GDPR and Article 14, paragraph 3, of the General Data Protection Regulation Implementation Act

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

2.3.1 GDPR

Pursuant to Article 83(1) of the GDPR, each supervisory authority shall ensure that the

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

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

Under paragraph 2, administrative fines shall be, according to the circumstances of the

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

measures referred to.

Date

November 26, 2020

Our reference

[CONFIDENTIAL]

It follows from the fourth paragraph, opening words and under a, that an infringement of the obligation of the controller pursuant to Article 32 of the GDPR is subject to a administrative fine 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, paragraph 3, 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 Regulation, impose an administrative fine not exceeding the in amounts referred to by these members.

3. Review

3.1 Processing of personal data

Since 19 October 2015, OLVG has been using a new and integrated hospital information system in which electronic patient records are stored.2 The data about patients that OLVG has in the hospital information system is processed information with which OLVG natural persons can identify. These patient data are therefore personal data within the meaning of Article 4, part 1, of the GDPR. Some 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 GDPR. Due to its scope, the term "processing" includes any possible operation or set of processing of personal data. Recording and consulting patient data in the hospital information system is also included. It concerns an extensive processing in which many 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 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, section 7, of the GDPR. The determining factor here is who has the purpose and means of processing the data personal data - in this case the processing of patient data in the hospital information system of the OLVG - determines. In order to answer this question, the AP in this case attaches value to the statements by 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 from 2015 and 2018.

2 On-site investigation dated 22 May 2019, Report 1: question 1.; Report 2: figures 2 to 7; Annual Report 2015 OLVG Foundation, p.16, 17;
Discussion report of the opinion session of 25 June 2020, p. 6.

3 Annual Report 2018 OLVG, p. 5-6.
https://www.olvg.nl/sites/default/files/jaarver Antwoording_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 a management merger has taken place in 2013 took place between the Sint Lucas Andreas Hospital foundation and the Onze Lieve Vrouwen foundation Gasthuis and that there has been one joint board since then.4 Subsequently, these two hospitals were closed in June legally merged into one hospital, named: Stichting OLVG.5 Furthermore, during the merger in 2015 introduced the current hospital information system uniformly within OLVG.6 This system is like mentioned above, finally put into use on October 19, 2015 by OLVG.7

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

hospitals, practices of medical specialists and medical day treatment centers, health centers and outpatient youth care.'8 OLVG further states 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 Precautions. 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 patient data and use of communication means' shows that OLVG has determined how OLVG employees have to deal with electronic patient files.10

On the basis of the above 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 electronic patient records from OLVG. This means that OLVG is the controller in the meaning of Article 4(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 infringing to the GDPR, the controller must, pursuant to Article 32 of the GDPR, processing inherent risks and take measures to mitigate risks. That measures should ensure an appropriate level of security, taking into account the status

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

5 OLVG Annual Report 2015, available at: https://www.olvg.nl/sites/default/files/jaarver Antwoording_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 from 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/jaarveroverzicht_2015.pdf, p. 4, last accessed: 30 July 2019.

7 “In October 2015 the joint electronic patient record (Epic) went live.”; Annual Report 2015 OLVG, available via: https://www.olvg.nl/sites/default/files/jaarverantwoording_2015.pdf, p. 17, last accessed: 30 July 2019; and article: https://www.medicalfacts.nl/2015/11/03/olvg-neemt-elektronisch-patientendossier-epic-in-uut/. Conversation report opinion session on 25 June 2020, p. 6.

8 OLVG East is the head office. Other locations 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 25 March 2019.

9 OLVG's response to AP information request dated May 3, 2019, appendix 8.

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

of the technology and the implementation costs compared to the risks and the nature of the personal data.11 In the following, the AP checks whether OLVG has an appropriate security level 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 put 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 for 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 for the use of the hospital information system of OLVG in two ways possible depends on whether access is requested from inside or outside the OLVG network.

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

from 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 username and password and no use is made of a staff card 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 on-site investigation. The regulators of the AP have this first observed during the demonstration of the hospital information system.14 This statement is also confirmed by the oral statements of [CONFIDENTIAL].15

Furthermore, during workplace inspections, the AP supervisors of three different employees16 of OLVG found that if the employee uses his/her username and enters the password correctly, he/she gains 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 the electronic patient records.

Furthermore, it is stated in article 2.1. of the 'Regulations on patient data and use of communication tools' 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 Workplace monitoring of [CONFIDENTIAL] (Report 6), one [CONFIDENTIAL] (Report 7) and one [CONFIDENTIAL] (Report 8).

17 On-the-spot investigation dated 22 May 2019, Reports 7 and 8, not at the [CONFIDENTIAL] (Report 6). See also the statement of

[CONFIDENTIAL] from OLVG, on-site investigation dated May 22, 2019, Report 2: questions 2 and 3.

18 OLVG response to AP information request dated May 3, 2019, appendix 28. This document states that it is effective from May 25, 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 found 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, log in to the VDI environment and the hospital information system with a username and password20 in combination with a varying token that is received or created by SMS or application.21

On 9 March 2020, OLVG linked a reader to every computer (terminal) and thus the above method changed. As a result, an employee must use his/her staff card for this reader and then enter a password before access to the computer can be obtained.22

3.3.2.2 Assessment

Pursuant to Article 32(1) of the GDPR, the controller must provide appropriate take technical and organizational measures to ensure a security level appropriate to the risk to ensure. In assessing the risks, according to Article 32, second paragraph, of the GDPR, attention must be paid to to be spent on risks that arise in the processing of personal data. As the data is more sensitive, or the context in which it is used presents a greater threat

affects the privacy of those involved, stricter requirements are imposed on the

data security.

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

This (usually) concerns extremely sensitive data about health. Health data is out

under Article 9(1) of the GDPR as a special category of personal data.

These personal data, which by their nature are particularly sensitive with regard to fundamental rights and

fundamental freedoms deserve specific protection as the context of their processing

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

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

to prevent infringements as much as possible.

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

for the privacy of those involved, OLVG had in

electronic health records must set up a two-factor authentication. The AP has in the

the foregoing, however, it has been established that employees can access a computer within the OLVG network

were able to access the data in the electronic patient records using only 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 has not used

a pass, token or other second factor. As a result, OLVG does not meet the requirement of at least

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

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

21 On-site investigation dated May 22, 2019, Report 2: authentication, question 4, figure 7-13.

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

Date

November 26, 2020

Our reference

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 in view of the current state of the technology and 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, prescribe two-factor authentication.

OLVG has further stated 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) current legislation and regulations, including the AVG. OLVG strives for it demonstrably comply with these standards.23 OLVG has thus also independently committed itself to comply with the above NEN standards, in which it is established that the identity of users must are established through two-factor authentication.24

Finally, the AP notes that, specifically with regard to the wording 'appropriate' technical and organizational measures' - as included in Article 32 GDPR - there is a continuation of what already applied under Directive 95/46/EC and the Personal Data Protection Act (Wbp).25 There is no question of a material change. Under those circumstances, it is obvious — also with a view to legal certainty — to continue with the interpretation followed in the past of Article 32(1) 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 is maintained.26 The AP has also always clearly communicated that the NEN 7510, if generally accepted security standard within the practice of information security in healthcare, remains an important standard for information security in healthcare under the GDPR regime and this guidelines must be followed.27

Opinion OLVG and response AP

In its view, OLVG states that the AP incorrectly judges that OLVG does not provide two-factor authentication has applied. According to Standard 9.4.1 of NEN 7510-2 (2017), health information systems that

process personal health information, identify users and this should be

to be done through authentication involving at least two factors.

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

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

personal staff card. The pass is configured in such a way that an employee 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, on the basis of Articles 3 and 5 of the Decree on electronic data processing by healthcare providers

obliged to ensure the safe and careful use of electronic devices 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, first paragraph, Directive 95/46/EC also already knew 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 See: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorggevers-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 no

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

is near the PC.

The AP does not follow OLVG's view. For an appropriate security of the personal data in electronic patient records, it is necessary that the OLVG information system only uses a two-factor authentication is accessible. If the access to the room is charged with an authentication via a personal card but the computer itself does not have two-factor authentication, then there is a greater chance that employees who are authorized to use the room (such as cleaners) but not 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 limited to the person holding a pass for a reader located near 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 AP is of the opinion that OLVG at least until 22 May 2019 Article 32, first paragraph, of the GDPR, now that OLVG's hospital information system has not complied with the requirement of two-factor authentication. OLVG has meanwhile terminated this violation by informing any computer(-terminal) to connect a reader. As a result, an employee must have his/her staff card in front of this reader and then enter a password before accessing the computer are obtained.

3.3.3 Logging check

3.3.3.1 Facts

OLVG's Information Security & Privacy Policy states that OLVG strives demonstrably comply with the standards NEN 7510 (information security in healthcare), NEN 7512 (base of trust for data exchange), NEN 7513 (logging actions on electronic patient records) and the AVG.28 In addition, OLVG indicates in the Epic Logging policy 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 preferably be identified early where necessary 30 To this end, all activities of users, systems and

information security events logged.31 From anomalous events

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

research.32 The Logging policy Epic distinguishes in the way in which the log data

are checked, i.e. randomly and on an incident basis.33

28 Research of 10 February 2020, appendix 2, item 3.3 and appendix 8, item 2.2.

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

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

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

32 Research of 10 February 2020, appendix 13, item 4.7.

33 Research of 10 February 2020, appendix 13, item 4.6.

Under Epic's Logging Policy, sample checks are required every four weeks

representative sample can be taken for analysis.34 The Epic Logging procedure shows that

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

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

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

sample.37 If there are major deviations for one or more users, then further

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

current events (based on an incident or a patient's request) give rise to this.39 Then the

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

the research question must come from Legal Affairs.40 From deviating events

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

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 act is

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

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

sample was taken

into the break-the-glass behavior of certain job groups.45 This applied to job groups

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

prepared on the basis of this sample consists of one page with figures and a graph of the

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 deviant 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 Research of 10 February 2020, appendix 13, under 4.6.

35 Research of 10 February 2020, appendix 14, item 3.4.

36 Research of 10 February 2020, appendix 14, item 3.4.

37 Research of 10 February 2020, appendix 14, item 3.4.

38 Research of 10 February 2020, appendix 14, item 3.4.

39 Research of 10 February 2020, appendix 13, item 4.6.

40 Research of 10 February 2020, appendix 13, item 4.6.

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

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

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

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

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

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

47 Survey 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 Survey of 10 February 2020, Annex 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
incidental checks also form a sample, since it is aggregated how
it often happens that there has been unlawful access and which incidents this concerns.51 According to the
[CONFIDENTIAL] of OLVG, very few irregularities were found in it and it constituted
no specific reason to schedule another sample.52 [CONFIDENTIAL] stated that
there is no random check every four weeks, as described in the logging policy
takes place, but that in practice it is looked at what gives rise to doing a
sample.53 The above samples are the only two samples that were performed.54 At the time
of the on-site investigation, an alarm was still being developed at certain limit values.55
In addition to these two random checks, OLVG also carried out incidental checks. OLVG has in the period
from January 2018 to April 2019, eight incident checks were carried out.56 This concerns the retrieval of
one electronic patient record at a time in response to a patient's request.57
As a result of the opinion session of 25 June 2020, OLVG issued additional information on 13 July 2020.
provided written documents, including a data query on all logging data, reports from
samples from different perspectives and reports arising from the newly applied

selection method.

3.3.3.2 Assessment

It has already been explained in section 3.3.2.2 that the controller pursuant to Article 32,

first paragraph of the GDPR must take appropriate technical and organizational measures to

risk-adjusted security level.

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

has 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

established that in the period from 1 January 2018 to 22 May 2019, OLVG did not carry out any systematic

has checks for conspicuous deviations of all logging of all electronic patient records

carried out, nor applied systematic or automatic alerts when exceeding

certain limit values in the logging whereby all logging of all electronic patient files

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, item 8.

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

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

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

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

56 Survey of 10 February 2020, Appendices 16 to 23.

57 Survey of 10 February 2020, Appendices 16 to 23.

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. The logging control has been in place since the investigation on the spot of the AP in May 2019 further tightened. As of 1 July 2019, OLVG has the frequency of the check on the logging already increased to once every two weeks (at least two or more reports per month). This check involves a (bi-weekly) data query on all logging data.
In the period from July 2019 to November 2019, reports are based on logging data made from different perspectives. From these different perspectives, during this period reported multiple times about the logging behavior. The different perspectives have also been used to determine where the risk of unauthorized access is greatest. It has started from May 2020 with a new selection method. All contacts are assigned a score with a higher score means a greater chance of unauthorized access. As of June 2020, there will be at least every two weeks made a printout of 50 views with the highest point score on a random day, which rated and then further investigated if suspected of illegality. In addition to the random check, ad hoc logging check takes place if the actuality (from the resolution incidents or at the request of a patient) gives rise to this. OLVG is of the opinion that this complies with standard 12.4.1 of NEN 7510-2 (2017).
As mentioned above, the AP has established that OLVG in the period from 1 January 2018 to 17 April 2019, two samples and eight incidental checks of the logging of one electronic patient file. OLVG thus 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. Apart from that, doing just eight occasional checks and two proactive samples in a period of 15.5 months amply and evidently insufficient to be able to speak of an appropriate security level that refers to signaling unauthorized access to patient data and taking measures in response to unauthorized access. In doing so, the AP of importance 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 (usually) this concerns:
highly sensitive health data. Stricter requirements are therefore 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 data subjects, OLVG therefore had the
log data regularly. In this way, unauthorized access can be signaled and
take action. The basic principle of the AP is that checking the logging systematically and
must take place consistently, whereby a random check and/or check based on
complaints is not enough. 58 The fine-grainedness of the authorization model used and the control of the
The correctness of the authorizations partly determines the intensity of the check on the logging. At a
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 assessment of
log files, which is in the context of this processing under Article 32 of the GDPR
requires. 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 files 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, regularly
prescribe logging.
Finally, OLVG has, 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 from
events that affect user activities, exceptions, and information security events
should be created, stored and regularly reviewed.

In view of the foregoing, the AP is of the opinion that OLVG at least until 22 May 2019 Article 32, first paragraph, of the GDPR because OLVG has not regularly reviewed log files. OLVG has this violation has now ended because they have completed the procedure with regard to the control of the logging tightened up and increased the frequency of checking the logging.

3.4 Other opinion OLVG and response from AP

3.4.1 Rights of the defense

OLVG argues that the imposition of a fine for the conduct observed by the AP is contrary to the nemo-tenetur principle59 as laid down in Article 48, paragraph 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 mentions that if during a procedure there is (the reasonable expectation) of a criminal charge, at least when it is not possible are excluded that the material will also be brought against the provider in connection with a criminal charge are used, the nemo-tenetur principle prevents it from being obtained in the procedure will-dependent material is used for an administrative punishment by means of fine.60

The fact that OLVG, pursuant to the Decree on electronic data processing by healthcare providers and the NEN standards contained therein is obliged to keep certain log files that monitor the makes compliance with the GDPR possible, according to OLVG does not mean that there is independence of will evidence. Pursuant to Article 33(1) of the GDPR, OLVG has on September 13, 2018 and on February 15, 2019 a report of a data breach was made to the AP. These data breach notifications concern according to OLVG information that does not exist separately from the will of OLVG: OLVG has compiled the information in order to comply with the obligation of Article 33(1) of the GDPR. Referring again to various court decisions, OLVG argues that will-dependent information may not be used for a administrative punishment by means of a fine.61 As a result of the two data breach reports launched an investigation as part of which the investigation was placed on May 22, 2019

59 The principle that no one is required to testify or confess against himself.

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;

HR July 12, 2013,

ECLI:NL:HR:2013:BZ3640;

61 HR 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.

By letter dated April 17, 2019, the AP furthermore, pursuant to Articles 5:16 and 5:17 of the General Act

administrative law (Awb) for information. The AP has not pointed out in this letter that OLVG is not

is obliged to provide information if doing so would prove a violation of the GDPR

to deliver. According to OLVG, this means that all information obtained by the AP with its request

for information, obtained under duress as referred to in Article 6(1) ECHR and Article 48(1)

member of the Charter. OLVG concludes that in view of the foregoing, the will-dependent information that

obtained under duress from OLVG cannot be used for the imposition of an administrative

fine.

Response 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, paragraph 1, of the European Charter and Article 6, paragraph 1, ECHR and the

closed nemo-tenetur principle has been obtained. Nor should evidence be excluded. AP motivates that as follows.

First of all, the AP will discuss the two data breach reports. As OLVG itself indicates, the two 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. Although the two data breach notifications 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 GDPR detected by the AP. Exclusion of those data breach reports as evidence is therefore not an issue. Apart from that, the AP considers the data breach notification as independent information. In view of Article 33, paragraph 5 of the GDPR, 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 this information.62

Secondly, the AP does not follow OLVG in its statement that the AP with its request for information of 17 April 2019 OLVG has been forced to provide information to the AP and as a result that information is not used may be used to impose an administrative fine. To this end, it is first relevant to establish that the AP requested information in that letter. No formal information has been 'claimed' under 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 letter in question refers to Article 58(1)(a) of the GDPR and article 5:16 jo. 5:17 Awb does not make this any different. Those references are for information only for OLVG in included the letter in order to make it clear that the AP (and its employees) OLVG to 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 (still) apply, that exclusion according to settled case-law applies only to evidence whose existence depends on the will of the

62 See, for example, also ABRvS 8 April 2020, ECLI:NL:RVS:2020:1011, ground for appeal. 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 received from OLVG in response to the information request from the AP dated May 3, 2019 both will-dependent 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 September 29, 2016 and reports of samples dated March 13, 2019 resp. March 26 2018. The AP subsequently did not use the will-dependent material to determine the violation and the imposition of the administrative fine. However, the violation is independent of will material, partly based on will-dependent material that was later provided by employees of OLVG after they have been informed of the right to remain silent by means of a warrant. Evidence exclusion is in the opinion of the AP is therefore not up for discussion.

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

3.4.2 Research objective

OLVG argues that the imposition of a fine for those identified by the AP conduct, at least with regard to authentication, is contrary to the rights of defence as laid down in Article 48, paragraph 2, of the European Charter and Article 6, paragraph 2, ECHR, since the observed behaviors fall outside the scope of the AP's earlier formulated research goal.

According to OLVG, the AP does not conclude in the investigation report that OLVG does not have an appropriate has taken technical and organizational measures to ensure that personal data

in the electronic health record cannot be 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, preamble, of the GDPR. A two-factor authentication as the AP enters it prevents
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 conduct to which the
saw data breach notifications. These employees would also use two-factor authentication such as the AP that
have had the authorization they currently have.

Response 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
GDPR, in order to ensure that personal data in the electronic health record are not
consulted by unauthorized employees. The AP has explicitly stated that the investigation
focuses on logical access security (authentication and authorization), logging, checking the
logging and awareness of employees.

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

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

The AP remarks unnecessarily that in its research goal it excludes the fact that personal data in the electronic health record may not be accessed by unauthorized personnel if mentioned guarantee. 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 significantly 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 checking on the logging do not stand alone, but must be considered in conjunction with all others appropriate measures. It is the combination of those measures that enables OLVG to to control the protection of personal data as well as possible and to prevent infringements as much as possible to prevent. Applying a two-factor authentication does not relieve OLVG of the obligation to promote employee awareness of patient privacy protection.

3.4.3 Interpretation of Article 32 of the GDPR

OLVG takes the position that the GDPR does not allow Member States and therefore the national legislator to offers to further flesh out the assessment against the standard of Article 32 of the GDPR by means of NEN-standards. According to OLVG, the AP is therefore acting in violation of the AVG by stating that in the investigation report to do. OLVG argues that only then can Member States go further than the regulation given protection, and may only elaborate on 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 GDPR not made by the AP, which is in conflict with the principle of due care. Finally, in the opinion of OLVG, the NEN standards cannot provide a basis for form for the implementation 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.

Response AP

The AP does not follow OLVG's view in this either. OLVG points to the prohibition of further (binding)
to set rules in national regulations in the event that a European regulation applies and this
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 explicitly does offer the
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, paragraph 3, of the UAVG
task assigned to monitor compliance with the GDPR - to the AP. That is what the AP
in the investigation report and what it is obliged to do.

When answering the question whether appropriate technical and organizational measures in the sense
of Article 32 of the GDPR, it is relevant what is included in the relevant NEN standards. This one
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 included in the
AVG
mentioned and created without being related to or based on the GDPR
the AP deems irrelevant. After all, Article 32 of the GDPR provides a standard that addresses all
controllers in all segments of the market. Referring to paragraphs 3.3.2 and 3.3.3
has the AP assessed whether OLVG has taken sufficient appropriate security measures such as
referred to in Article 32 of the GDPR, "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. In making that decision, the AP has the presence

of generally accepted security standards such as the NEN standards also in consideration

taken and allowed to take.

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

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 AVG.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 concludes from this that OLVG is also of the opinion that this

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

In the investigation report of the AP, reference is made to Article 3, second paragraph, of the Decree

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

healthcare 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

exchange system to which it is connected. OLVG states that the AP only pays a fine or an order

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

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

UAVG. Pursuant to Article 51 of the UAVG, the Wbp expired on 25 May 2018. This is also the basis

of the Begz will expire on that date.

Response AP

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

explained, the AP has imposed an administrative fine for the violation of Article 32, first paragraph, 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, on the basis of the Begz, it is obliged to comply with the standards

NEN 7510 and NEN 7512.

63 Research of 10 February 2020, appendix 2, item 3.3 and appendix 8, item 2.2.

64 Research 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 failing to meet the requirement of two-factor authentication and regularly reviewing log files.

The AP makes use of its authority to impose a fine on OLVG for the violation that has been established pursuant to Article 58, second paragraph, preamble and under i and Article 83, fourth paragraph, of the GDPR, read in conjunction with article 14, paragraph 3, of the UAVG. The AP uses the Fines Policy Rules 2019.65

After this, the AP will first briefly explain the penalty system, followed by the motivation of the fine in the present case.

4.2 Fine policy rules of the Dutch Data Protection Authority 2019

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

The AP has established fine policy rules regarding the interpretation of the aforementioned power to imposing an administrative fine, including determining the amount thereof.

Pursuant to Article 2, under 2.1, of the Penalty Policy Rules, the provisions with regard to violation

of which the AP can impose an administrative fine of up to the amount 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
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 statutory
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 Stcrt. 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 (up 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 GDPR and referred to in the Policy Rules under a to k.
4.3 Fine amount
4.3.1. Nature, seriousness and duration of the infringement
Pursuant to Article 7, opening words and under a, of the Fine Policy Rules 2019, the AP takes into account the nature,
the seriousness and duration of the infringement. In its assessment, 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 data

suffered damage 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 those data. Also to prevent unauthorized access to or use of personal data and the equipment used for the processing. The The controller must therefore, pursuant to Article 32(1) of the GDPR, provide appropriate and take technical and organizational measures to ensure a security level 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 of interest: these factors determine the potential damage for the individual data subject in the event of, for example, loss, alteration or unlawful processing of the data data. 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 established that, until at least May 22, 2019, OLVG will provide personal data without appropriate data processed security. This personal data contains highly sensitive information from patients of 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 unnecessarily 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, partly under the Wbp under which an appropriate level of security was already required, the AP considers serious. That it is also a processing of particularly sensitive data, an insufficient security of the personal data extra.

In view of the nature, seriousness, scope and duration of the infringement, the AP sees reason to increase the basic amount of the fine pursuant to Article 7, opening words and under a, of the Fine Policy Rules to be increased by €80,000 to €390,000.

4.3.2 Blame and negligent nature of the infringement

Pursuant to Article 5:46, second paragraph, of the Awb, when imposing an administrative fine, the AP

into account the extent to which this can be blamed on the offender. Now that this is a

violation, the imposition of an administrative fine in accordance with established case law does not require that it is demonstrated that there is intent and the AP may presume culpability if it offense is established. In addition, pursuant to Article 7, under b, of the Fine Policy Rules 2019 into account the intentional or negligent nature of the infringement.

OLVG is obliged under Article 32 of the GDPR to implement security measures that are appropriate for the nature and scope of the processing operations carried out by OLVG. Now OLVG for longer period no two-factor authentication and regular checking of the log files in her organization, the AP is of the opinion that OLVG is in any case particularly negligent failed to take such measures. OLVG is allowed, partly in view of the sensitive nature and due to the large scope of the processing, it is expected that it complies with the standards that apply to it identified and acted upon. The AP considers this culpable.

In addition, OLVG has indicated in its own Information Security & Privacy Policy that 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 AVG. OLVG strives for this demonstrably complying with these standards. OLVG has further stipulated in its logging policy that for the checking the log data takes a representative sample every four weeks for analysis. It

The AP considers that the fact that OLVG also does not comply with its own existing policy rules is very negligent. It had located 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, the detection of 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 adjust the basic amount of the fine on the basis of of Article 7(b) of the 2019 Fine Policy Rules 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 to a disproportionate outcome. The AP is of the opinion that, given the seriousness of the violation and the extent to which in which this can be blamed on OLVG, the (height of) the fine is proportional.66 The AP does not see any reason the amount of the fine on the basis of proportionality and the other in Article 7 of the Fines Policy Rules mentioned circumstances, to the extent applicable in the present case, to increase or decrease.

4.4 Conclusion

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

66 See paragraphs 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 GDPR amounting to € 440,000 (in words four hundred and forty thousand euros).67

Yours faithfully,

Authority Personal Data,

w.g.

drs. C.E. Mur

board member

Remedies Clause

If you do not agree with this decision, you can return it within six weeks of the date of dispatch of the decide 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 effect 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 paper submission is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague.

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

In your notice of objection, write at least:

- your name and address;
- the date of your notice of objection;
- the reference mentioned in this letter (case number); or attach a copy of this decision;
- the reason(s) why you do not agree with this decision;
- your signature.

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