Registered mail

[CONFIDENTIAL]

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

Date

January 15, 2020

Our reference

z2019-17017

Contact

[CONFIDENTIAL]

Your letter from

July 29, 2019 (your reference: 232958)

Topic

Decision on objection regarding fine and order subject to penalty Haga Hospital

Dear [CONFIDENTIAL]

You hereby receive the decision of the Dutch Data Protection Authority (AP) on your objection of 29 July 2019 and supplemented by letter and fax dated 10 September 2019. The objection is directed against the decision of the AP of June 18, 2019 (reference: z2019-07604) to impose an administrative fine as well as an order to your client Haga Hospital Foundation (Haga Hospital). The decision of June 18, 2019 hereinafter (also) referred to as the primary decision.

1.

Course of the procedure

1. On 4 April 2018, the AP received a report of a data breach from HagaZiekenhuis.

2. As a result of the aforementioned report, the AP has launched an investigation. In that context, on 31

October 2018 an on-site investigation at Haga Hospital took place.1

3. The investigation resulted in a report of preliminary findings in January 2019. On that

Haga Hospital responded in writing on 4 February 2019.

4. The AP - with due observance of Haga Hospital's response - subsequently submitted the investigation report

definitively adopted and forwarded to HagaZiekenhuis by letter dated 26 March 2019.

1 With regard to the course of the investigation, reference is made to p. 2 and 3 of the primary decision as well as to paragraph

1.2, p. 4

of the AP's final investigation report referred to below.

Annex(es) 1

Date

January 15, 2020

Our reference

z2019-17017

5. In a letter dated April 4, 2019, the AP intends to impose an administrative fine and/or order

sent to Haga Hospital under penalty. Haga Hospital has both

in writing (by letter dated 18 April 2019) and orally (during a hearing on 25 April 2019) her

point of view.

6. Taking into account the view of HagaZiekenhuis, the AP has decided by decision of 18 June 2019

to impose both an administrative fine and an order subject to a penalty for violation of

Article 32(1) of the GDPR.

7. In a letter and fax dated 29 July 2019, HagaZiekenhuis lodged an objection on grounds to be further stated

against the aforementioned decision and requested a period of 6 weeks to supplement the grounds.

8. In a letter dated 31 July 2019, the AP gave HagaZiekehuis the opportunity no later than 11 September 2019

to supplement the grounds of objection.

9. By letter and fax dated September 10, 2019 as well as by letter and fax dated October 4, 2019 HagaZiekenhuis supplemented its grounds for objection.

10. On October 16, 2019, a hearing was held at the offices of the AP. Of hearing is a report made. This report is annexed to this decision.

11. On October 17, 2019, an on-site investigation took place at the offices of Haga Hospital in The Hague to check whether Haga Hospital has complied with the order subject to a penalty.

12. As a result of what was transacted during the hearing on October 16, 2019, HagaZiekenhuis informed letter, fax and e-mail dated 5 November 2019 further detailed her appeal to limited financial capacity substantiated.

13. In a letter dated 2 December 2019, the AP informed Haga Hospital that Haga Hospital at the time of the on-site investigation of October 17, 2019 met the burden. 2

14. By letter dated December 5, 2019, the AP asked you whether the aforementioned letter from the AP dated December 2, 2019 there is reason for Hagaziekenhuis to withdraw the grounds for objection against the order subject to a penalty. In In response to this, you indicated in a letter dated 13 December 2019 that Haga Hospital has no reason to sees its grounds for objection with regard to the order subject to periodic penalty payments.

2 Earlier, in a letter dated 22 August 2019, the AP already concluded that HagaZiekenhuis, when implementing the of 9 August 2019 (reference: 2019/0177/CvdW/PM/rv) the intended measures mentioned are met with the load element that relates to the checking of log files. In letters from Haga Hospital dated 24 and 30 September 2019 (reference: 2018/0109x/CvdW/PM/cb and 2018/0109z/CvdW/JP/rv respectively), HagaZieknhuis explained how it implements given to the burden.

Date

January 15, 2020

Our reference

z2019-17017

2.

Legal framework

15. The relevant legal framework is included as an appendix at the end of this Decree.

3.

The primary decision

16. Pursuant to Article 58, second paragraph, preamble and under d and i, in conjunction with Article 83, fourth paragraph, opening words and
under a, of the General Data Protection Regulation (GDPR) and Article 14, paragraph 3, of the
Implementation Act General Data Protection Regulation (UAVG), the AP is (among other things) authorized to:
impose an administrative fine and an order subject to periodic penalty payments with regard to infringements of the GDPR.

17. In the primary decision, the AP issued an administrative fine and an order to HagaZiekenhuis
penalty imposed for violation of Article 32, first paragraph of the GDPR, read in conjunction with
Article 3, second paragraph, of the Decree on electronic data processing by healthcare providers and the
determined under 12.4.1 of NEN 7510-2 because the requirement of two-factor authentication is not met and the
requirement to regularly review the log files.

18. The amount of the administrative fine has been set at €460,000. In doing so, the AP based itself on the
Fines Policy Rules of the Dutch Data Protection Authority 2019 (Fines Policy Rules 2019).3

19. Article 32 GDPR is, as follows from Article 2.3 of the Fines Policy Rules 2019, classified in category II.
A fine range of € 120,000 – € 500,000 and a so-called basic fine of
€310,000. This basic fine serves as a (neutral) starting point for the further determination of the
amount of the fine.4 The AP then adjusts this further provision to the factors described in Article 7 of the
Fines Policy Rules 2019. This allows the basic fine to be increased or decreased.

20. In the primary decision, the factors from Article 7, opening words and under a (nature, seriousness and duration of the infringement) and b (intentional/negligent nature of the infringement), of Article 7 of the Fines Policy Rules 2019 de
reason to increase the fine twice by € 75,000.

21. In addition to an administrative fine, HagaZiekenhuis was also subject to an order subject to a penalty due to

the same violation. The charge is that Haga Hospital - within fifteen weeks of the date primary decision - to allow access to its hospital information system solely with application of two-factor authentication, and that the log files are regularly checked for unauthorized access or use of patient data. The amount of the penalty is set at € 100,000 for every two weeks after the end of the beneficiary period, up to a maximum amount of €300,000 in total.

3 Stcrt. 2019, no. 14586, March 14, 2019.

4 The amount of the basic fine can be calculated by dividing the minimum and maximum amount of the relevant bandwidth and then divide by two (cf. art. 2.4 Fines Policy Rules 2019).

Date

January 15, 2020

Our reference

z2019-17017

4.

Grounds for the objection

22. In summary, HagaZieknhuis has put forward the following grounds for objection.

No grounds for enforcement of NEN standards

Lack of legal basis for enforcement

23. HagaZiekenhuis believes that the AP has no legal basis for taking enforcement action. Otherwise than the AP suggests, it follows neither from the GDPR nor from the Additional Provisions Processing Act personal data in healthcare (Wabvpz) that the obligation to take 'appropriate measures' should be are completed on the basis of NEN standards 7510, 7512 and 7513. Reference is made to these standards in Article 3, paragraph 2 and Article 4 of the Decree on electronic data processing by healthcare providers (Begz).

24. The power to lay down further rules for the processing of . for a particular sector

personal data (Article 26 Wbp) has lapsed with the introduction of the AVG. It follows that
the disappearance of the basis of the Begz, namely Article 26 Wbp, not (exclusively) with Article 15j
Wabvpz could be recovered. After all, this means that no authority has yet been granted to the AP to
specific rules for a particular sector. The Wabvpz is therefore not an elaboration of the GDPR, but
stands on its own, alongside the GDPR and its predecessor, the Wbp. The AP is not authorized to take enforcement action
due to an alleged violation of the NEN standards on the basis of the Begz/Wabvpz. To this end, only the
Health and Youth Care Inspectorate authorized.

25. It follows from paragraph 2.4 of the explanatory memorandum to the UAVG that the material standards for
data processing directly from the GDPR and should no longer be done at national level
fixed. The AP can therefore not fill in the open standards in the GDPR with national laws and regulations
regulations, by means of NEN standards. Haga Hospital refers to considerations 8, 10 and 13
of the preamble to the GDPR. The GDPR requires the Member States to provide an autonomous interpretation. The AP can
therefore not impose a fine or order subject to periodic penalty payments on the basis of the (U) AVG for violation of the
NEN standards.

Contrary to the principle of legality

26. HagaZiekenhuis is also of the opinion that the contested decision is contrary to the principle of legality.

27. The AP can only take enforcement action due to violation of the provisions of Article 32 of the GDPR
included open standard. At the time of the alleged violation, this standard was according to Haga Hospital
not further specified. From the principle of legality laid down in Article 7 ECHR and Article 5:4(2) Awb
it follows that the AP could not take enforcement action. A sanction can only be imposed because of a bee or
conduct prohibited by law. In addition, in view of the lex certa-
principle to be sufficiently clear, foreseeable and knowable. That is not the case here, according to Haga Hospital
case because the content of the open standard in Article 32(1) of the GDPR could not be known by a concrete
application in practice. The AP should have clarified this open standard first. The reference of the

Date

AP to a report from the Dutch Data Protection Authority from 2013 is of no help to the AP because this report is based on the Wbp and the NEN standards.

28. Also the mere fact that HagaZiekenhuis has taken the NEN standards as a starting point in its policy, does not mean that the AP can enforce compliance on the basis of the (U) AVG. Article 5:4, paragraph 2 Awb requires a legal basis. Internal policy is insufficient.

29. Insofar as it may be tested against the NEN, HagaZiekenhuis argues that the AP has failed to clarify when 'regular review of log files' is involved.

During the opinion session, Haga Hospital explained how the monitoring of the logging within Haga Hospital is taking place and has explicitly asked the AP for a concrete interpretation of the standard. That should have been a reason for the AP to make this standard more concrete. The AP's argument in paragraph 5.2 of the contested decision, in which it substantiates why it has not given any interpretation to the standard 'regularly', therefore does not hold, because it means that the need for the size of controls depends on the way in which controls are carried out. And the AP knew the method of control.

30. Haga Hospital finds the NEN-7510-2 so vague that it conflicts with the legality and principle of legal certainty cannot be enforced by means of a fine or an order subject to a penalty.

31. In its letter dated October 4, 2019, HagaZiekenhuis further motivated why it believes that the GDPR does not provide scope for further detailing Article 32 of the GDPR by means of NEN standards. She refers in doing so based on case law of the Court of Justice of the EC from which it follows that Member States have no provisions, may add substantive rules or binding interpretative provisions to a regulation.5 The AP According to HagaZiekenhuis, it does this by applying the NEN standards (which are national standards). This stands in the way of a uniform application of the GDPR in the EU. The GDPR has no provision that makes it possible to set further national rules with regard to Article 32 GDPR.6

Objections to the amount of the fine and the amount of the penalty payment

Haga Hospital has not been negligent

32. Haga Hospital states that it was not negligent. In this regard, she points out the following affected measures:

o An extra warning is displayed when an employee opens a file;

o There is a mandatory e-learning course for all employees who have access to the electronic patient record;

o All employees are informed in a personal letter of professional secrecy and the importance of confidentiality of patient data;

o Additional information is provided at the introductory meeting for new employees;

o The employment contract has been tightened;

5 ECJ 18 February 1970 (Bollmann, 40/69), ECJ 6 July 1972 (Schlüter & Maack) ECJ 10 October 1973 (Variola, 34/73) and ECJ 31 January 1978 (Fratelli Zerbone, 94/77).

6 In that context, HagaZiekenhuis refers to the judgment of the ECJ on 11 January 2001 (Azienda Agricola Monte Arcosu, C-403/98).

Date

January 15, 2020

Our reference

z2019-17017

o There is an option for patients to additionally shield their patient data;

o Where possible, authorizations are tightened;

o A customized solution is being developed for checking the logging.7

33. Haga Hospital further indicates that the conclusion that she was negligent is incorrect because the AP goes beyond that implementing two-factor authentication is not a measure that prevents unauthorized access in patient records by employees. After logging in with two-factor authentication,

after all, it is still possible for employees to look in a patient file without authorization.

34. HagaZiekenhuis also notes that the statement of the AP that the victim affected by HagaZiekenhuis measures do not refer to the regular checking of the logging, is not correct. Haga Hospital has, as laid down in the report of the opinion session, the number of samples increased from four to six.

In this regard, HagaZiekenhuis further notes that it is in conflict with the principles of proper administration in general and the principle of legal certainty in particular to impose an administrative fine based on an unclear standard (the NEN standard with regard to logging is open) and that standard has not been specified by the governing body.

AP wrongly fined Haga Hospital twice

35. The AP imposed a basic fine of € 310,000 on Haga Hospital. This basic fine has been AP subsequently increased twice with an amount of € 75,000 because, according to the AP, there is "a structural violation that continues to this day". The AP's substantiation for the first increase of the basic fine amounts to the same as the substantiation for the second increase. The continuous violation established by the AP is after all the result of the fact that Haga Hospital has taken no or insufficient measures. According to Haga Hospital it is not in accordance with the Fine Policy Rules and it is also not reasonable to double the basic fine increase because of the same fact. The double increase is therefore also contrary to the ne bis in idem rule. principle (Article 5:43 Awb).

Fine wrongly not reduced

36. Article 7, preamble and under c, of the Fine Policy Rules gives the AP the option to set the basic fine decrease if measures have been taken by the controller to reduce the to limit the damage suffered by those involved. In this regard, Haga Hospital draws attention to the measures taken.

37. The fine imposed by the AP on Haga Hospital is directly at the expense of the (scarce) resources that can be used for patient care. This means that the fine is at the expense of the possibility to

invest in care and innovate, on the basis of which Haga Hospital remains able to provide sustainable care

7 This customized solution (a software application specially developed for Haga Hospital called [CONFIDENTIAL]) is implemented and active. Did they refer to the letter from Haga Hospital of 24 September 2019 (reference: 2018/0109x/CvdW/PM/cb) as well as to the letter from the AP of 2 December 2019 containing the findings as a result of the on-site investigation on October 17, 2019 to verify compliance with the charge.

to deliver. Haga Hospital also believes for this reason that a reduction in the basic fine is justified is.

38. Finally, Haga Hospital invokes reduced financial capacity and requests that reason for fines. In this regard, HagaZiekenhuis points out in its letter of 5 November 2019 a report from the audit firm [CONFIDENTIAL] and a report from the financial strategic consultancy [CONFIDENTIAL], and refers them further to the financial figures of HagaZiekenhuis about 2019.

Penalty sum set too high

39. The AP has attached a penalty of € 100,000 for every two weeks that is not (entirely) the charge has been met, up to a maximum amount of € 300,000 in total. Haga Hospital sets itself up on the take the view that these amounts are disproportionate to the alleged conduct. With that, the decision is conflict with the principle of proportionality within the meaning of Article 3:4 Awb and also with the specific provision in Article 5:32b, paragraph 3, Awb.

40. The order subject to a penalty is at the expense of the possibility to invest in healthcare and to innovate. That cannot be the purpose of enforcement. Haga Hospital also believes for this reason that a reduction of the penalty is justified.

41. The amount of the penalty is contrary to the principle of equality. The AP has since the

various orders subject to periodic penalty payments were imposed upon the entry into force of the GDPR. The penalty that

Haga Hospital is imposed is by far the highest.

42. The penalty payment is contrary to the principle of proportionality, because one penalty amount is linked to

a load that consists of two parts. This means that Haga Hospital also forfeits penalty payments if

part 1 is complied with, but part 2 is not. According to Haga Hospital, this is unreasonable.

5.

Verdict AP

43. Haga Hospital processes electronically and on a large scale in its hospital information system

(medical) personal data. This (usually) concerns extremely sensitive data about health. This one

qualify data as a special category of personal data within the meaning of Article 9, first paragraph,

GDPR to which, in principle, a processing ban applies unless there is an exception as stated

in the GDPR and UAVG. It is very important for patients' trust in a healthcare provider that

these personal data are handled with the utmost care and that they are adequately secured.

Hospital patients - who are often in a vulnerable position - must always be able to access it

confidence that their personal data will be treated confidentially and that

employees who do not have a treatment relationship with the patient or who do not need data for the

management handling of the care or treatment, unauthorized patient files may be

consult. Against this background, the AP conducted an investigation at Haga Hospital. In response to

of the results of that investigation, it was established in the primary decision that HagaZiekenhuis no, then

has not taken adequate technical and organizational measures as referred to in

Article 32, first paragraph, of the GDPR and an administrative fine and an order subject to a penalty has been imposed. In
The AP comes to the present decision on the objection as a result of the
grounds for objection do not lead to a different opinion.

Appropriate measures; two-factor authentication and logging control

44. The violation of Article 32(1) of the GDPR involves two aspects. The first concerns non-compliance with
the requirement of two-factor authentication. It has been found that for users of the
hospital information system was able to access the data in the digital
patient records containing only something a user knows (namely a username and password).
In that case, one-factor authentication is used.8 The hospital information system of
Haga Hospital did not have the built-in obligation, but only the option to use two-factor
login authentication. As a result, Haga Hospital did not correctly meet the two-factor requirement
authentication implemented in its business operations.9 This has also been recognized by HagaZiekenhuis.10

45. The second reason why Article 32(1) of the GDPR has been infringed is related to failure to regularly
checking the logging of access to patient records. Logging means that a
care institution structurally keeps track of who consulted which patient file and when, so that
unauthorized access can be detected and action taken if necessary. It
Haga Hospital's policy provided for a check on the logging of a random sample of annually
six patient records.11 In the relevant period covered by the AP's investigation - January 2018 to
with October 2018 - proactively there has been one check on unauthorized access12 and 6 checks on
request from patients and staff.13 14

46. □□One check in the period from January 2018 to October 2018 can be compared with the number
patient visits 15 that Haga Hospital receives annually and in 2017 (rounded up) came to 381,50016 and the

8 In general, three factors are distinguished: something the user knows (a password or PIN); something that
the user has (for example, a token); or something that the user is (a biometric metric). (Source: NCSC, Use
two-factor authentication. Passwords alone are not always enough. Factsheet FS-2015-02, version 1.1. October 22, 2018).

9 Cf. p. 11, section 2.3 AP investigation report, March 2019

10 See the Letter Haga Hospital 4 February 2019 (reference: 2018/109j/CvdW/PM/rv), p. 2 under the heading 'Authentication' and also report
of the hearing following the notice of objection, p. 6. Since September 30, 2019, Haga Hospital applies the two-factor authentication correctly. (Cf. letter Haga Hospital 30 September 2019 (reference: 2018/0109z/CvdW/JP/rv).

11 Letter HagaZiekenhuis, 23 October 2018 (reference: 2018/0109c/RdF/PM/rv), answer to question 5 and Appendix 3: Digital authorization
Patient Records.
Haga Hospital (version 1.0, May 2018), p. 3 and 6.

12 With regard to the file of the well-known Dutchman.

13 Cf. letter HagaZiekenhuis, 23 October 2018 (reference: 2018/0109c/RdF/PM/rv), answer to question 5.

14 At present the number of samples is 132 per year. For more information, see the report of findings from December 2, 2019 to
following the on-site investigation into compliance with the order subject to penalty on October 17, 2019.

15 Which visits always result in consultation of a patient file.

16 In 2017, there were 381,500 patient visits. cf. the appendix to the letter Haga Hospital of 9 August 2019 (reference: 2019/0177/CvdW/PM/rv). The AP also refers to the figures from the Annual Report submitted by HagaZiekenhuis for the opinion hearing.
This concerns a total of (rounded off) 381,500 patient visits in 2017, which are subdivided into 28,500 admissions, 158,000 first outpatient clinic visits, 52,000 first aid consultations and 143,000 nursing days.

number of employees who (potentially) have access to patient records17, in the opinion of the AP not be regarded as a 'regular' check and therefore not as an appropriate measure in the sense

of Article 32(1) of the GDPR. In addition, the AP notes that the Haga Hospital
performed reactive checks either - independently or in combination with the proactive check of
the patient file of the famous Dutch person - can be regarded as regular checks.
After all, such reactive checks depend solely on an (explicit) request from a
patient or employee.18

47. Also the six (proactive) checks on the logging that Haga Hospital announced19 and performed20
in 2019, the AP, again compared to the number of patient visits - which always result in
consultation of a patient file21 - and the number of staff, insufficient to be considered regular
can be designated.

Consistent explanation of 'appropriate measures' under the Wbp and the GDPR

48. Both the requirement of two-factor authentication and the requirement of checking the logging are not new. It's alright
to continue the way in which also under the old regime of Directive 95/46/EC and the Wbp
what was seen as 'appropriate measures' has been implemented and has been derived from the NEN standard
7510-2.22 The AP has continued this explanation in the context of the interpretation of Article 32, first paragraph, GDPR and
has always been transparent about this.23 The DPA is of the opinion that this explanation is also a
is a correct interpretation of the standard 'appropriate measures' from Article 32(1) of the GDPR. Because
Haga Hospital has not acted in accordance with this explanation, the AP finds the imposition of enforcement
appropriate measures. After this, the AP will state its position against the background of the objections of
Motivate Haga Hospital in more detail.

6.

Reconsideration

49. Pursuant to Article 7:11 of the Awb, the AP assesses on the basis of your objection whether it
has rightly proceeded to the imposition of the order subject to periodic penalty payments and an administrative fine.

17 During the hearing (p. 6 hearing report), Haga Hospital stated that 3,500 people are employed at
HagaHospital.

18 The AP notes in this regard that the check carried out by HagaZiekenhuis is also not in accordance with its own

authorization policy.

19 Statement [CONFIDENTIAL], 31 October 2018 as reflected in the report of official acts dated 19

December 2018, appendix 3, page 4-5 and Haga Hospital response dated 23 October 2018, appendix 19: Procedure Sample

Logging and

Planning Sample Logging.

20 Report of the opinion session. P.2, which report is attached as an appendix to the letter from the AP dated May 16, 2019

(reference: z2019-07604).

21 A sample of 6 related to 381,000 patient visits (and with that at least as many file consultations) then comes

down to 0.0016 %.

22 In June 2013, the AP published an investigation report on this; https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-

care-institutions-careless-with-medical-data

23 Cf.: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorggevers-en-de-avg?qa=nen%207510&scrollto=1

en

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorggevers-en-de-avg#welke-norm-hanteert-de-ap-als-het-

concerns-the-security-of-patient-data-7366.

Date

January 15, 2020

Our reference

z2019-17017

Jurisdiction, Article 32 GDPR and lex certa

Jurisdiction

50. Haga Hospital states that the AP can only impose a fine and an order subject to a penalty

base on the basis of the AVG and the UAVG and not on the basis of the Wabvpz and the basis thereof

Begz, with the NEN standards included therein.

51. The AP notes the following in this regard. It was established in the primary decision that Haga Hospital de

(security) standard as laid down in Article 32, first paragraph, of the GDPR because insufficient
appropriate technical and organizational measures have been taken to ensure a risk-adjusted
level of security for the processing of personal data. So it's out of that norm
Article 32, first paragraph, of the GDPR, which the AP has found to have been infringed by
Haga Hospital.24 Although the primary decision considers that Article 32 of the GDPR in
coherence must be read with Article 3, second paragraph, of the Begz and the provisions under 12.4.1 of
NEN 7510-2, but the conclusion cannot be drawn from this that the Begz or the NEN standards
are regarded as the violated regulations on the basis of which the AP proceeded to impose
of enforcement measures.25 That is not the case either. In the present case, however, the NEN
7510-2 contained the requirement for two-factor authentication as well as the requirement to regularly review log files
assessment, the concrete interpretation/interpretation of what in this case is considered 'appropriate technical and
organizational measures" within the meaning of Article 32(1) of the GDPR apply. The AP has the
fine and the order subject to periodic penalty payments therefore also not imposed on the basis of and because of a violation
of the
Wabvpz and/or the Begz and the NEN standards included therein, but on the grounds of not taking
appropriate technical and organizational measures within the meaning of Article 32(1) of the GDPR.
52. In its notice of objection, supplemented by letter of 4 October 2019, HagaZiekenhuis further points out
European law case law26 □□This case law essentially refers to the prohibition to
to set (binding) rules in national regulations in the event of a European regulation. A
however, such a situation does not arise in the present case. No further rules have been set. That doesn't take away
that Article 32 GDPR must be applied and interpreted in a specific case. The application and
interpretation is - in view of the task assigned to it in Article 6, paragraph 3, UAVG to supervise
GDPR compliance - to the AP. That is what the AP has done and what it is bound to do.
It is ultimately up to the national court and the Court of Justice of the EU to assess whether the AP
24 On the basis of Article 58, second paragraph, opening words and under d and i, of the UAVG, in conjunction with Article 83,
fourth paragraph, opening words and under a,

of the GDPR and Article 14, paragraph 3, of the UAVG, the AP is authorized to impose an administrative fine and an order subject to a penalty

if there is a violation of Article 32, first paragraph, of the GDPR.

25 In this regard, the AP notes, moreover, that Haga Hospital is bound by the Begz and therefore, in view of Article 3, second paragraph,

Begz, is legally obliged to comply with the NEN standards mentioned therein. That, according to HagaZiekenhuis in its notice of objection, the

authority to lay down further rules for a certain sector for the processing of personal data (Article 26 Wbp) with the

The introduction of the AVG has lapsed, the AP contradicts. In the opinion of the AP, Article 6, second paragraph and or third paragraph,

AVG, expressly the possibility to do so.

26 ECJ 18 February 1970, case 40-69 (Bollmann), ECJ 6 June 1972, case 94-71 (Schütler & Maack), ECJ 10 October 1973, case 34-73

(Fratelli Variola), ECJ 31 January 1978, case 94/77 (Fratelli Zerbone)

Date

January 15, 2020

Our reference

z2019-17017

interpretation of the standards from the GDPR that it has given is legally correct.27 This means that a autonomous interpretation.

Article 32 GDPR and lex certa

53. With regard to HagaZiekenhuis's assertion that the primary decision is in conflict with the principle of legality contained the lex certa principle because - as HagaZiekenhuis argues - there would be a vague standard, the AP considers as follows.

54. The lex certa principle requires the legislator to provide legal certainty in such a

describes a norm or prohibited behavior in the clearest possible way.28 Someone must be able to know in order to for what conduct or omission he may be punished. This requires that the implementation of a legal provision must be sufficiently clear, specific and known. However, that does not mean that the use of a vague or open standard is not possible. On the contrary, the legislator can suffice with such standards. Open standards can be necessary and therefore acceptable because the law must also be able to function in changed circumstances.29 In the so-called Krulsla judgment, the Supreme Court that, when describing crimes, it is necessary to make use of a certain vagueness, consisting in using general terms, is sometimes unavoidable to prevent behaviors that being punishable fall outside the scope of the description of the offence.30 It is not always possible to provide for how the interests to be protected will be violated in the future and because, if this is provided, crime descriptions are otherwise too refined, with the result that the clarity disappears and thus harms the interest of the general clarity of the legislation. In addition to the The Supreme Court also interprets the lex certa principle in this way by the (supreme) administrative judges.31

55. With regard to the question of whether the relevant standard from Article 32(1) of the GDPR (the obligation to of 'appropriate technical and organizational measures') conflicts with the lex certa principle, notes the AP the following.

56. First of all, according to the text of Article 32(1) of the GDPR, the measures to be taken must take into account take into account the state of the art, the implementation costs, as well as the nature, scope, context and the purposes of the processing and the risks of varying likelihood and severity to the rights and freedoms of persons. Furthermore, in Article 32, first paragraph, preamble, and parts a-d, GDPR made a further specification of what the 'appropriate technical and organizational measures' among others includes32:

27 Cf. House of Representatives, session 2017–2018, 34 851, no. 3, p. 53

28 The lex certa principle is laid down in Article 5:4 Awb, Article 7 ECHR and Article 15 ICCPR as well as Article 49 of the Charter of the fundamental rights of the European Union.

29 ECHR, Kokkinakis vs. Greece, Judgment of 25 May 1993, 14307/88.

30 HR, judgment of 31 October 2000, ECLI:NL:HR:2000:AA7954, para. 3.4.

31 See, for example, ABRvS 9 July 2014 (ECLI:NL:RVS:2014:2493), CBb 22 February 2012 (ECLI:NL:CBB:2012:BV6713) and CRvB 8 January 2019

(ECLI:NL:CRVB:2019:26).

32 Article 32 GDPR includes a more specific elaboration of the (general) principle of integrity and confidentiality such as laid down in Article 5, first paragraph, preamble and under f, GDPR.

a) the pseudonymisation and encryption of personal data;

58. b) 59. the ability to maintain confidentiality, integrity, availability and resilience on an ongoing basis

of the processing systems and services;

61. c) 62. the ability, in the event of a physical or technical incident, to control the availability of and access to the

restore personal data in a timely manner;

64. d) 65. a procedure for regular testing, assessment and evaluation of effectiveness

of the technical and organizational measures to secure the processing.

The second paragraph of Article 32 GDPR further states that when assessing the appropriate

security level takes into account, in particular, the processing risks resulting from

unauthorized access to data transmitted, stored or otherwise processed, either by

accident or unlawful.

57. Thus Article 32 of the GDPR, also in conjunction with the preamble33, already provides a further explanation of the standard

‘appropriate technical and organizational measures’ and it is indicated that specifically

must be kept. This includes "ensuring integrity"34 and "unauthorized"
access'35. The requirements of two-factor authentication and regular checking of the logging form a
further elaboration/definition of those concepts. In light of the foregoing, in the opinion of
the AP, requiring two-factor authentication and regular monitoring of logging in the context of the
taking appropriate technical and organizational measures to prevent unauthorized access
prevent or impede, then also reasonably foreseeable. It must be considered
that Article 32 of the GDPR provides a standard that is addressed to all controllers, regardless of in
which market segment they are active. The GDPR therefore targets all areas and all forms of
to cover data processing. All controllers must therefore comply with this standard
(can) take. Furthermore, the measures to be taken must be in accordance with the state of the art
Technic. In order to be able to implement this in a meaningful way, it is necessary to prescribe those
measures are not possible in view of the speed with which technology in today's highly digitized
society progresses. With the rapidly developing technology, a new
consideration must (can) be made. This requires (a certain degree of) flexibility and
future-proofing of the standard, and that justifies that – against the background of the above

33 Recital 83 in the preamble to the GDPR is textually very similar to what it says in Article 32 GDPR:
In order to ensure security and to prevent processing from infringing this Regulation, the
controller or the processor assess the risks inherent in the processing and take measures, such as
encryption, to mitigate those risks. Those measures should provide an appropriate level of security, including
including confidentiality, taking into account the state of the art and the implementation costs
compared to the risks and the nature of the personal data to be protected. When assessing the
data security risks, attention should be paid to risks arising from
personal data processing, such as the destruction, loss, alteration, unauthorized disclosure of or
unauthorized access to the data transmitted, stored or otherwise processed, either accidentally or
unlawful, which can lead in particular to physical, material or immaterial damage.

34 Article 32, first paragraph, preamble and part b, GDPR.

35 Article 32, second paragraph, GDPR.

Date

January 15, 2020

Our reference

z2019-17017

cited case law listed under paragraph 52 – in this case it is (more) open
standards as included in Article 32 of the GDPR.36

58. With regard to the question whether the explanation given by the DPA to the standard 'appropriate technical and organizational measures' is sufficiently clear, determined and known, the following is further from interest. In general, the material standards to which the processing of personal data under the GDPR regime, have broadly remained the same as those under the Directive 95/46/EC and the Wbp.37 Specifically with regard to the terms 'appropriate technical and organizational measures' - as included in Article 32 GDPR - there is a continuation of which also applied under Directive 95/46/EC and the Wbp.38 There is no question of a material change. below those circumstances, it is obvious – also with a view to legal certainty – that the to continue the interpretation followed in the interpretation of Article 32, first paragraph, GDPR. This means that the already in past implementation through the requirements of two-factor authentication contained in the NEN standards and regular assessment of the log files is maintained.39 It is also always clear by the AP disseminated that the NEN 7510, as a generally accepted security standard within the practice of the information security in healthcare, an important standard for information security under the AVG regime in healthcare and these guidelines must be followed.40 In a similar sense, the AVG Helpdesk for Healthcare, Welfare and Sport communicated this. 41

59. In view of the above, the AP is of the opinion that the European legislator has been able to suffice with the standard laid down in Article 32 GDPR with regard to the appropriate technical and organizational measures.

A closer look at the 'regular check' standard

60. Specific with regard to the requirement of regular monitoring of the logging and the objection of
Haga Hospital that this standard is too vague, the AP additionally notes the following. The AP belongs to
believes that the (proactive) monitoring of the logging in the period from January 2018 to October 2018

36 In this context, the AP also refers to the explanatory memorandum to Article 13 of the Wbp (the predecessor of Article 32 of the GDPR): (…)"In the
The term <<appropriate>> implies that the security is in accordance with the state of the art. This is primarily a
question of professional ethics of persons charged with information security. The standards of this ethics are set forth in this provision
provided with a legal final piece, in the sense that a legal obligation for the controller is attached to it. It is
not for the legislator to provide further details about the nature of the security. Such details would be highly time-bound and thereby undermining the desired level of security. "(…). (underline added by the AP). See TK 1997-1998, 25
892, no. 3, p. 98-99.

37 It is apparent from recital 9 in the preamble to the GDPR that the objectives and principles of Directive 95/46/EC remain intact.

38 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.

39 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

40 Cf.: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorggevers-en-de-avg?qa=nen%207510&scrollto=1 en
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorggevers-en-de-avg#welke-norm-hanteert-de-ap-als-het-concerns-the-security-of-patient-data-7366

41 See: https://www.avghelpdeskzorg.nl/onderwerpen/veiligheid/nen-7510. This helpdesk is a collaboration between

umbrella organizations in healthcare, the social domain, NOC*NSF and the Ministry of Health, Welfare and Sport.

13/32

Date

January 15, 2020

Our reference

z2019-17017

of one file (related to the file of the well-known Dutchman)42 compared to the 381.50043 patient visits and associated file consultations at the Haga Hospital in 2017 (evidently) not as can be qualified as 'regular'. This also applies to the - at the time of the imposition of the administrative fine announced44 and partially implemented45 - random check on the logging of six files for 2019. The idea behind it is that sufficient attention is paid to the information in the number of patients and staff present in the hospital. This generates a processing of very large amounts of data. Haga Hospital has to deal with a large number of patient visits and has a lot of employees who (potentially) can all gain access to patient files.46 The ‘open’ considering the nature of a hospital (anyone can visit a hospital; well-known and unknown patients), the sensitivity of the personal data and the fact that good care was provided should be made so that access to - and thus the processing of - medical data does not may be an obstacle, makes (correctly) that a regular check on the logging that is in proportion to the number of files and file consultations is necessary for good security. A (manual)
In the opinion of the AP, sample of 6 patient files does not show a sufficient sense of urgency and does not indicate that Haga Hospital is 'in control' in this area. Haga did not have a automatically organized checking process, but used a manual check that also performed on a very occasional basis. As mentioned, this method does not match well with the large number of patient visits/file consultations and the associated risk of potentially unauthorized file consultations. In the opinion of the AP, it is therefore not possible to speak of an appropriate measure. Haga Hospital should also have realized this and should have been clear in view of the standard that the

AP also used before the entry into force of the GDPR. Viewed against that background is of a too

vague/unclear standard, as HagaZiekenhuis states, is out of the question.

61. That the AP did not indicate in advance how many files in the case of Haga Hospital did

should be assessed does not mean that, as HagaZieknhuis argues, the standard

vague and there is a violation of the principle of legality or legal certainty. How much

files must be assessed, partly depends on the facts and circumstances of the

concrete situation, such as the number of logging in relation to the number of patient files and the number of

employees that can get access, and can therefore be different on a case-by-case basis. In addition, the AP notes that it is

quantifying in advance what is 'regular', often not easily possible and/or desirable because that

may affect the level of protection required in a specific case. This would, partly in view of

the time-bound nature of the state of the art, the ability to respond in a timely manner to

changing circumstances and future developments, the application of the regulations in high

may hinder. For example, it is not inconceivable that in the near future it will be possible to

by means of, for example, specific software applications in a simpler way and on a larger scale

42 For more details on the factual findings with regard to the logging, see the investigation report of the AP of March 2019, p.

13 and 14 with

including references to the relevant sources.

43 For an explanation of this number, see further appendix (section 2.1) to the letter from HagaZiekenhuis dated 9 August

2019 (reference:

2019/0177/CvdW/PM/rv).

44 See appendix (par. 2.1) to the letter from HagaZiekenhuis dated 9 August 2019 (reference: 2019/0177/CvdW/PM/rv).

45 P. 15 (top) of the primary decision.

46 During the hearing (p. 6 hearing report), Haga Hospital stated that 3,500 people are employed at

HagaHospital.

assess files on logging. The software now used by Haga Hospital

[CONFIDENTIAL] for the purposes of logging control confirms this position.47

More is expected from professional parties

62. Finally, in connection with the above - superfluously - the following is noted. For a

successful appeal to the lex certa principle is made by professional parties, such as Haga Hospital, more

then expect from non-professionals. When it comes to professional parties, it may be required that they

have an insight into the meaning of (open) norms addressed to them and, if necessary, allow themselves to be properly

inform them about the restrictions to which their behavior is subject.48 This is all the more pressing now that the

concerns the processing of health data, which, as stated, qualify as a special

category of personal data and for which, in principle, a processing ban applies, unless there is

a ground for exception and extra guarantees have been taken care of. It was on the road from

Haga Hospital, if it was unclear about this, to verify the explanation if necessary

of Article 32 GDPR by means of the two-factor authentication contained in the NEN standards and

regular checks on the logging.

63. In addition, the AP emphasizes that HagaZiekenhuis itself was very aware of the measures to be taken on the ground

of Article 32 of the GDPR. The AP concludes that from the assessment made by Haga Hospital itself in

its authorization policy, entitled 'Authorisation of Digital Patient Records'. Haga Hospital makes

explicit mention of the security obligation in the AVG and it is noted that healthcare providers

must fulfill this obligation by applying the existing NEN standards, including NEN

7510.49

Conclusion lex certa

64. In view of the foregoing, the AP concludes that there is no question of a violation of the lex certa principle

is. The objection in this regard is unfounded.

Two-factor authentication and unauthorized access

65. Haga Hospital states that the measure of two-factor authentication is not a measure that

(completely) access to patient files by employees.

66. In this regard, the AP notes first of all that this does not alter the fact that this measure - as before

explained with reasons - one of the obligatory measures to be taken is appropriate within the meaning of Article 32

of the AVG and HagaZiekenhuis must therefore also take this measure. In addition, the AP notes that the

two-factor authentication is a concrete (care-specific) control measure that, together with other

control measures, the purpose of which is to prevent unauthorized access to systems and applications as much as possible

47 For more information about this software, see the letter from HagaZiekenhuis dated 24 September 20189 (reference:

2018/0109x/CvdW/PM/cb) as well as the

letter from the AP dated December 2, 2019.

48 Cf. HR, judgment of 31 October 2000, para. 3.5 (ECLI:NL:HR:2000:AA7954), HR, judgment 18 January 2005, para. 3.4

(ECLI:NL:HR:2005:AR6579),

CBb 18 December 2018, para. 5.3.2 (ECLI:NL:CBB:2018:652).

49 Version 1.0, May 2018, p. 3, under the heading 'c. Security obligation', as well as version 2.0 of that document, which is part

of Annex 2

is part of the 'Final report Investigation into unlawful access to patient file' of May 2018 (reference: 20180412ISO01).

Date

January 15, 2020

Our reference

z2019-17017

that this measure, as Haga Hospital states, is not a measure that guarantees that

unauthorized access to patient records by employees no longer occurs, does not alter the fact that the

is a measure that contributes significantly to the prevention of unauthorized access. In this

framework, the AP emphasizes that applying two-factor authentication - and also the control of the logging -

does not stand alone, but must be viewed in conjunction with all other appropriate ones to be taken
measures. It is the combination of those measures that makes Haga Hospital able to
to control the protection of personal data as well as possible and to control infringements as much as possible
to prevent.

International value NEN standards

67. In its notice of objection, Haga Hospital also refers to the national character of the NEN
standards. Applying a national standard would hinder the uniform application of the GDPR in the EU
stand.

68. With regard to this ground for objection, the AP first of all notes that - as above under marginal
52 even though it has been noted - is obliged to monitor compliance with the GDPR and in that context in a
specific case must also explain the standards included in the GDPR, even if it concerns more
open standards as laid down in Article 32 GDPR. The AP did that in the primary decision and
in this decision through the requirement of two-factor authentication and the requirement to regularly
judge. This does not mean that (in advance) there is a situation that is contrary to a
autonomous interpretation of the GDPR. Whether this explanation stands in the way of the uniform application of the GDPR,
can
may be submitted, if desired, to the national court and (ultimately) to the European Court of Justice
Justice.

Apart from that, the AP notes the following. The relevant NEN standards in this case concern the
Dutch rendering of the European and international standard NEN-ISO / IEC 27002+C1+ C2:2015 en
NEN-EN-ISO 27799:2016 (en).51 These standards have been developed in an international context at
ISO(International Organization for Standardization) or IEC(International Electrotechnical
Commission). ISO and IEC together form a body of bodies specializing in global
normalization. National organizations that are members of ISO or IEC participate in developing
International Standards through technical committees established by the appropriate organization
for standardization in specific technical fields. ISO and . technical committees

IEC collaborate on topics in which they have a common interest. Others

international organisations, both public authorities and NGOs, are taking, in collaboration with ISO and IEC,

also participate in this work. In the field of information technology, ISO and IEC have a

Joint Technical Committee established, ISO/IEC JTC 1.

The documents - and the standards contained therein - that have been accepted by the Netherlands are subsequently

the NEN-ISO or NEN-IEC coding. Standards with the coding: NEN-EN-ISO are European accepted.52

50 Cf. par. 9.4.1, p. 57, NEN 7510-2:2017

51 NEN 7510-2, foreword, p. 7.

52 Cf.: https://www.nen.nl/Normontwikkeling/Wat-is-normalisatie/European-en-international-norms.htm

Date

January 15, 2020

Our reference

z2019-17017

In short, the relevant NEN standard is therefore about standards that are applied at international and European level

are accepted and used.53

Amount of the fine and penalty payment

69. HagaZiekenhuis puts forward various objections that, in its opinion, should lead to

fines. These are discussed below.

Negligent culpability

70. HagaZiekenhuis states that it has not been negligent and points to the measures it has taken.

71. With regard to this ground for objection, the AP notes that, notwithstanding the

measures taken, Haga Hospital should also have taken other measures to ensure an appropriate

to ensure a level of security. As set out in the primary decision, the negligent

culpability for not using two-factor authentication and not regularly checking

the log files. Those measures should also have been taken, and with regard to those

measures, the AP accuses Haga Hospital of negligence. To that extent, those measures are therefore independent of the measures taken by HagaZienkenhuis.

72. The AP has substantiated why the number of random samples carried out by HagaZiekenhuis was less than for the purpose of checking the logging (evidently) cannot be regarded as 'regular' control" and is therefore contrary to Article 32 of the GDPR. That the AP does not have in advance in that regard indicated how many samples are sufficient does not mean that, as Haga Hospital argues, because of conflict with the general principles of good administration or the principle of legal certainty, an administrative fine could not have been imposed.54 Also the argument of Haga Hospital that manual checking is very time-consuming does not mean that Haga Hospital would thus be relieved of the obligation under Article 32 of the GDPR and would therefore suffice with a sample of six files. In addition, the AP points out with regard to Haga Hospital's statement that it is manually checking is time-consuming, on the capabilities of specific software applications that make this important extent can be overcome. The AP believes that it would have been located on the road from Haga Hospital here to show initiative earlier by acting actively and adequately.

Ne bis in idem

73. HagaZiekenhuis further argues that it wrongly has twice increased the basic fine occurred. According to HagaZiekenhuis, the justifications for these increases are the same down. And in the opinion of HagaZiekenhuis, that is in violation of the fine policy rules of the AP and with the ne bis in idem principle contained in Article 5:43 Awb.

53The text of ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015 has been prepared by the Technical Subcommittee ISO/IEC/JTC 1/SC 27 “Information security” of the International Organization for Standardization (ISO) and the International Electrotechnical Committee (IEC) and has been adopted as EN ISO/IEC 27001: 2017. (See the “European foreword” on p. 1 of the document NEN-EN-ISO/IEC 27002:2017).

54 In this regard, the AP also refers to what has been considered about this in paragraph 57.

74. The AP cannot follow HagaZiekenhuis in its argument and considers the following in this regard. The AP has in the primary decision increases the basic amount of the fine on the basis of two factors. this fine increasing factors are contained in Article 7, under a and b, of the Fine Policy Rules and are derived from Article 83, second paragraph, under a and b, of the GDPR.55

75. The first increase of the basic fine by € 75,000 on the basis of the factor 'nature, seriousness and duration of the infringement'

(Article 7(a) of the Fines Policy Rules) is on the one hand related to the nature and seriousness of the violation and, on the other hand, with the duration of the violation.

With regard to the nature/severity it is important that it concerns the lack of two suitable (fundamental) security measures, namely a mandatory two-factor authentication56 and the regularly checking and reviewing log files. In addition, the seriousness of the violation further colored by the number of employees who have had unauthorized access to the relevant patient record57, the number of patients included in the hospital information system,58 the type personal data (health data) contained therein as well as the trust of hospital patients that are greatly shamed by this.

In addition to the aforementioned nature and seriousness, the duration of the violation also contributed to the (first) increase of the basic fine by € 75,000. In that regard, it is important that the violation existed since at least case January 2018 and had not yet ended at the time of the imposition of the fine on June 18, 2019.

76. The second increase of the basic fine by € 75,000 is based on Article 7, opening words and under b, of the Penalty Policy Rules. It is an increase due to the negligence of Haga Hospital. Despite that the management of Haga Hospital was aware of the unauthorized inspection of the file concerned, has it wrongly seen no reason in this to take measures in good time to ensure a correct implementation of the use of two-factor authentication and regular checking of the

log files. In that regard, the AP notes that the argument of

lack of time is not a legitimate argument to refrain from taking security measures and thus

allow the violation to continue.59 In the opinion of , the aforementioned circumstances justify

the AP the second increase of the basic fine by € 75,000.

77. In conclusion, the AP notes that the reason for the first increase in the basic fine is different from that

for the second increase. The increases are based on various factors from the GDPR and the

Fine policy rules that are taken into account when determining the amount of the fine. Of a

There is therefore no question of double fines and the ne bis in idem principle does not apply here. It

The objection raised in that context is unfounded.

55 The AP is obliged to take these factors into account when determining the amount of the fine in a specific case.

56 The hospital information system does not have the built-in obligation, but only the possibility to use two-factor

login authentication.

57 According to Haga Hospital's own research 'Final report Investigation of illegal access to patient file' of May 2018, (p. 27

at the top) it concerns 85 employees of Haga Hospital who unlawfully had access to the patient file of the

famous Dutchman. See also AP Research Report March 2019, p. 4.

58 As noted earlier, this concerns a total (rounded off) of 381,500 patient visits in 2017.

59In this regard, the AP refers to the Guidelines WP 253, which cites as an example for the “negligent nature of the

infringement”:

failure to apply technical updates in a timely manner (WP 253, 2016/679, p.12).

Fine moderation

78. Haga Hospital is of the opinion that there is a circumstance that reduces the fine as referred to in

Article 7, opening words and under c, of the Fine Policy Rules because of the measures it has taken to:

limit the damage suffered by those involved.

79. The AP does not follow HagaZiekenhuis in its argument and considers as follows. Article 7, opening words and under c, of the Fine Policy Rules gives the AP the option to reduce the basic fine if the

controller has taken measures to prevent the damage suffered by the data subjects

to limit. The measures taken by HagaZiekenhuis are aimed at complying with the

Haga Hospital under Article 32, first paragraph, of the GDPR, but lead to the

In the opinion of the AP, the AP does not admit, or insufficiently, that the damage suffered by those involved has been limited. In

In this connection, the AP notes that Haga Hospital with regard to the two-factor authentication and the

control on the logging, after they have been set as a result of the Haga Hospital itself

investigation was aware of the unauthorized access and subsequently by the AP in the final

investigation report of March 2019 also pointed out the violations found60,

has made insufficient efforts to take sufficient appropriate measures in a timely manner. The AP also sees

no reason to mitigate the fine imposed on the basis of Article 7, opening words and under c, of the

Penalty Policy Rules.

80. According to HagaZiekenhuis, there is also a reason for fines to be mitigated because the fine is directly at the expense

of the (scarce) resources that could otherwise have been used for patient care, as well as at least

the expense of the ability to invest and innovate. In this regard, Haga Hospital also has

expressly invoked reduced capacity and has expressed its position in this regard

substantiated with two reports in which various hospitals, including Haga Hospital,

[CONFIDENTIAL] and [CONFIDENTIAL] were assessed for their financial health.61

81. In this too the AP sees no reason to moderate the fine. When determining the height of the

administrative fine, pursuant to Article 5:46, second paragraph, of the Awb, account must be taken of the

proportionality principle. In that regard, the administrative authority must, if necessary, take into account

the circumstances under which the violation was committed. From the parliamentary history at the Awb

it appears that the carrying capacity can be such a circumstance.62 This is also the case in case law
confirmed.63

82. It follows from case law that if it appears on the basis of financial data submitted by the offender
that the offender is disproportionately affected by the fine, the amount of the fine must be moderated.64 The
However, the AP does not consider the financial situation of HagaZiekenhuis to be such that it should be taken into account

60 P. 14-15 of the AP Investigative Report, March 2019.

61 It concerns the reports [CONFIDENTIAL].

62 Parliamentary Papers II, 2003/04, 29 702, p. 141.

63 ABRvS 21 March 2012, ECLI:NL:RVS:2012:BV9508 and HR 28 March 2014, ECLI:NL:HR:2014:685.

64 See ABRvS 12 March 2008, ECL I:NL:RVS:2008:BV9509.

concluded that Haga Hospital is disproportionately affected by the amount of the fine and
fine moderation due to reduced financial capacity is indicated. The AP has hereby presented the annual accounts of
2018 as well as the information provided by HagaZiekenhuis in a letter dated 5 November 2019 and
further documents.65

83. The operating result of € 622,892 for the 2018 financial year is not such that HagaZiekenhuis de
cannot bear a fine of €460,000. The return for 2019 is now forecast at
€947,00066 In addition, it appears from the annual accounts that HagaZiekenhuis had access to
€ 24,011,362 in freely available liquid assets.67 68 The circumstance that [CONFIDENTIAL] the
financial health of HagaZiekenhuis - in the context of a benchmark in which they measure the financial
position of Dutch general hospitals - has assessed with a 4 (2017)
and a 569 (2018) because its return is below the 2% norm and also below the market average of

1.48%, Haga Hospital cannot benefit either. While the AP acknowledges that the financial situation of
Haga Hospital compares worse with other hospitals, this does not mean that
Haga Hospital is insufficiently financially sound to bear the fine imposed on it. The AP considers the
argumentation presented by HagaZiekenhuis in view of the financial resources it has at its disposal
insufficient to mitigate the fine in view of the ability to pay principle. The same goes for the
assessment of [CONFIDENTIAL] which has the return and EBITDA70 of Haga Hospital
assessed.

84. That the fine is directly at the expense of (scarce) resources that would otherwise be used for other purposes
could have been deployed, the AP acknowledges and endorses Haga Hospital's statement that
the scarce resources of a hospital should in principle be spent on care. Nevertheless, this can
Haga Hospital's argument in this case is of no avail. The protection of personal data must also be done in a
be properly anchored in the daily practice of a hospital where
worked with special personal data. In addition, following the lecture of Haga Hospital
ultimately result in a healthcare institution not being able to be fined at all.

Charge under penalty

Haga Hospital meets the burden

65 In that regard, the AP notes that, pursuant to Article 38 of the UAVG, the effect of the decision imposing an administrative fine
shall be suspended until the term of appeal has expired or, if an appeal has been lodged, until a decision has been made on the appeal. Moreover
Article 4:94 Awb offers the possibility to make a payment arrangement.

66 Letter to Haga Hospital of 5 November 2019, p. 2.

67 See Annual Report 2018 HagaZiekenhuis Foundation, 5.1 Annual Accounts, par. 5.1.5 Notes to the balance sheet as at 31 December 2018, p. 17.

68 Unnecessarily, the AP also refers to the advice from 2016 of the predecessor of the European Data Protection Board in which the

indicated that controllers and processors cannot infringe data protection law

legitimize by claiming a shortage of resources. See WP 253, 2016/679, p.12.

69 On a scale of 1 to 10.

70 EBITDA is the abbreviation of Earnings Before Interest, Taxes, Depreciation and Amortization. It is used as a measure of

the

profit that a company earns from its operating activities without incurring costs and revenues from financing

processed. See: https://nl.wikipedia.org/wiki/EBITDA.

Date

January 15, 2020

Our reference

z2019-17017

85. Haga Hospital indicates that it maintains its objection with regard to the order subject to a penalty,

notwithstanding the letter from the AP dated December 2, 2019 in which the AP states that the charge has been met.

She points out that in that letter the AP makes a reservation with regard to compliance with the order

in the future.

86. The AP notes the following in this regard. The conclusion of the aforementioned letter states that71:

The AP concludes that at the time of the on-site investigation of October 17, 2019, Haga Hospital was

complied. It should be noted that the verification process with [CONFIDENTIAL] is dynamic and on

subject to change. The business rules used in conjunction with [CONFIDENTIAL] serve

to be continuously improved. This improvement should be part of the PDCA improvement cycle."

The above quote states that it appears that Haga Hospital complied with the requirement. At this time

there is no reason to judge otherwise. In short, Haga Hospital meets the burden. What the

AP wanted to make clear with the aforementioned passage about the verification process with [CONFIDENTIAL],

is that the way in which the mandatory control of the logging should take place - as a consequence of the

obligation to take appropriate measures pursuant to Article 32 GDPR - is dynamic in nature. That keeps

connection with the time-bound nature of the state of the art, and the possibility to
be able to respond to any changed circumstances and future developments (see also
for this marginal number 57). Against this background, Haga Hospital is based on the resting on it
obligation under Article 32 GDPR to continuously monitor the control process and, if necessary,
improving, specifically when it comes to refining the business rules. That is independent of the
observation that Haga Hospital currently meets the burden. However, what now becomes appropriate
considered, this may no longer be the case in the (near) future. It is also for this reason that it is required
that controllers go through the PDCA improvement cycle in order to - in order to comply with Article 32
GDPR and at the time Article 13 Wbp - to ensure a permanently appropriate level of security in the organisation
guarantees.72 That is what the AP wanted in its letter of 2 December 2019 to Haga Hospital
information, but that does not detract from the fact that the AP is of the opinion that Haga Hospital
meets the load. It is true that, as the AP also indicated in its letter of 2 December 2019,
the order subject to penalty has not been lifted and can re-examine in the (near) future whether the order
is still complied with. This follows from Article 5:34, second paragraph, of the Awb.73

Height penalty; principle of equality and proportionality

87. HagaZiekenhuis also takes the position that the amount of the penalty payments is disproportionate
uphold the alleged conduct. According to HagaZiekenhuis, the contested decision is therefore in conflict with
the principle of proportionality within the meaning of Article 3:4 Awb and also with the specific provision in Article

71 Letter AP dated December 2, 2019, p. 8.

72 In its guidelines of February 2013, the CBb explained at the time what appropriate measures entail. This one
guidelines are still up-to-date and useful in this regard. See: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-
publishes-guidelines-security-of-personal

73 In the present case, termination will only be considered if HagaZiekenhuis makes a request to that effect on the basis of
Article 5:34 Awb.

5:32b, paragraph 3 Awb. In the opinion of the AP, this ground for objection is in vain and considers as follows in this regard.

88. Provided that Haga Hospital has complied with the order and no penalty payments have been forfeited. For that reason, the AP does not see in what interest HagaZiekenhis still has in the grounds for objection put forward with regard to the order subject to penalty. Apart from that, the AP notes the following.

89. The amount of the penalty must be in reasonable proportion to, on the one hand, the gravity of the interest violated by the violation of the statutory regulation and, on the other hand, the intended effective operation of the penalty. It is important that the penalty payment has such an incentive must assume that the imposed order is complied with and forfeiture of the penalty is prevented. The AP is of the opinion that in this case a periodic penalty payment has been imposed whereby there is a reasonable relationship in the aforesaid sense and considers as follows.

90. With regard to the gravity of the interest violated by the violation of the statutory provision the AP emphasizes that it concerns extremely sensitive data about health. This data qualify, as stated several times, as a special category of personal data within the meaning of Article 9, first paragraph, GDPR, to which, in principle, a processing ban applies unless there is an exception such as stated in the AVG and UAVG. It is important for patients' confidence in a healthcare provider It is important that these personal data are handled with the utmost care and that they are protected in terms of security meet the highest standards. In that context, it should be noted that the present case concerns the lack of two fundamental security measures and that, despite the fact that the management of Haga Hospital was aware of the unauthorized inspection of the file in question, there was no reason for this wrongly has seen to take timely measures to ensure the correct implementation of the handling of two-factor authentication and checking the log files regularly. These circumstances therefore, in the opinion of the AP, justify the amount of the penalty payment as set out in the contested

decision have been made.

91. HagaZiekenhuis is of the opinion that the determined penalty payment is contrary to the principle of equality and points in this regard to charges previously imposed by the AP, in which lower penalty payments have been established. This one

In the opinion of the AP, the ground for objection is without purpose and explains that position as follows.

92. In a general sense it should be noted that the mere circumstance that the penalty payment in the case of Haga Hospital would be the highest compared to penalties imposed by the AP earlier, does not mean that the penalty in this case is too high or contrary to the principle of equality. The amount of a penalty is assessed and determined on a case-by-case basis, taking into account all relevant circumstances of the specific case.

93. With regard to the periodic penalty payments imposed on other care providers in 200974, and to which Haga Hospital refers to the principle of equality, the AP notes that these cases were from a relatively distant past (now ten years ago) - they took place in a different

74 Those cases involved periodic penalty payments of €1,000 and €2,000 per day, with maximum amounts of €30,000 and €60,000.

Zeitgeist and predate the GDPR - and where there were violations of a distinctly different earth. It concerned non-compliance with obligations of a (mainly) administrative nature, such as: failure to perform a risk analysis, failure to prepare a risk analysis report information security or a job profile information security officer, appoint/appoint an information security officer and a portfolio holder information security. In the case of Haga Hospital, two fundamental security measures are involved

- two-factor authentication and regular logging - which have not been applied. Moreover, in the case of Haga Hospital precedes a serious security incident, which also clearly changes the context used to be. It is equally important in this regard to note that the Dutch DPA - the predecessor of the AP - earlier in 2013, after research at various healthcare institutions, found that no provision was made for sufficient appropriate measures with regard to access to patient records (treatment relationship) and regarding the control of the logging.75

94. With regard to the penalty payment in the case of the National Police, and where HagaZieknhuis points out that in that case it concerned a penalty of € 50,000 per two weeks, the AP notes that in that case it is one violation and not two as in the present case. This circumstance makes the difference in the imposed penalty payments can be explained in the opinion of the AP. In addition, the maximum amount of €320,000 in the case of the National Police comparable. Finally, it should be noted that in the case of Haga Hospital has actually experienced a serious security incident.

95. In addition to the foregoing and to illustrate the case-specific nature of the height of a The AP still refers to the order subject to a penalty imposed on VGZ in 2018. The height of the penalty there amounted to €150,000 per week and with a maximum of €750,000, due to the fact that employees of VGZ actually had access to personal health data while that was not necessary for their work (without it being established that this employees have actually consulted this data).76 It follows from this that the AP also has higher imposes periodic penalty payments in a case that is comparable in important respects to the present order under penalty.

96. According to HagaZiekenhuis, the penalty payment that has been determined is still contrary to the principle of proportionality because one penalty amount is linked to an order that consists of two parts, which also means penalty payments are forfeited if the first part of the order is, but the second part of the load is not carried out. The AP cannot follow Haga Hospital's position and notices it next on.

97. In itself there is no obligation to pay the order subject to periodic penalty payments on the proposed by HagaZiekenhuis way, and according to the AP there is no reason to do so in this case. The at Haga Hospital imposed burden concerns the implementation of two measures, both of which are related to compliance with the obligation to take appropriate security measures pursuant to Article 32 GDPR. To both

75 https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-patientendossiers-binnen-healthcare institutions.pdf

76 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_last_onder_dwangsom_vgz.pdf

obligations must be met in order to ensure that Article 232 GDPR is complied with. It concerns a cumulation of measures that together ensures that, in accordance with Article 32 GDPR is being acted upon. Even if one of these obligations is not met, it is still there is a violation of Article 32 GDPR. It is about achieving that simultaneously fulfilled all obligations arising from the duty to take appropriate measures.

98. Finally, HagaZiekenhuis points out the enormous challenge of HagaZiekenhuis to remain financially healthy remain and argues that the cease and desist order comes at the expense of the ability to invest and innovation in healthcare. According to HagaZiekenhuis, that cannot be the intention of enforcement and that justifies a reduction of the penalty, according to HagaZiekenhuis. The AP follows the argument of Haga Hospital is not and is considering as follows.

99. The order subject to a penalty must provide such an incentive that the order imposed is carried out without a penalty being forfeited.77 It is not related to this position that when determining the penalty payment takes into account the circumstance that the forfeiture of the penalty payment is at least at the expense of the possibility to invest and innovate in healthcare because then the incentive to

burden to perform is removed too much. In this regard, the AP draws a comparison with the statement of the Administrative Jurisdiction Division of the Council of State of 6 February 201978 from which it follows that a penalty that would be determined according to ability to pay, does not provide sufficient incentive to the offender to end burden. It also follows from previous case law that the financial circumstances of the In principle, the offender (may not) play a role in determining the amount of the penalty.79 The AP also considers the ground for objection put forward by HagaZiekenhuis in this regard as an appeal to such financial circumstances and is of the opinion that in this case they should not play a role in the determination of the amount of the penalty.

Conclusion

100.

Pursuant to Article 7:11, first paragraph, of the General Administrative Law Act, the AP contested the decision reconsidered in response to the objections raised. In this review, the AP assessed whether it has rightly decided to impose a fine and an order subject to a penalty.

101.

In view of the foregoing, the AP is of the opinion that when making the primary decision, it is right has proceeded to the imposition of the fine and order subject to periodic penalty payments. There is also no question of a change of relevant facts and circumstances since the primary decision, so that there is no reason to revoke the primary decision and make a different decision.

77 See, for example, ABRvS 10 July 2019 (ECLI:NL:RVS:2019:2343), ABRvS 12 June 2019 (ECLI:NL:RVS:2019:1870) and ABRvS 17 April 2019 (ECLI:NL:RVS:2019:1243).

78 ECLI:NL:RVS:2019:321.

79 ABRvS 26 October 2016 (ECLI:NL:RVS:2016:2797).

Date

January 15, 2020

Our reference

z2019-17017

25/32

Date

January 15, 2020

Our reference

z2019-17017

dictum

7.

The Dutch Data Protection Authority declares the objection unfounded.

Yours faithfully,

Authority Personal Data,

mr. A. Wolfsen

Chair

Remedies Clause

If you do not agree with this decision, you can return it within six weeks of the date of dispatch of the decision to submit a notice of appeal to the court pursuant to the General Administrative Law Act (sector administrative law) in the district in which you are domiciled. You must provide a copy of this decision to send along.

26/32

Date

January 15, 2020

Our reference

z2019-17017

APPENDIX

Legal framework

General

Pursuant to Article 7:11 of the General Administrative Law Act (Awb), the AP assesses on the basis of your objection whether it has rightly decided to reject your GDPR complaint in the primary decision. The reconsideration takes place (in principle) taking into account all facts and circumstances as they are at the time of the review.

GDPR

Article 32 Security of processing

1. Taking into account the state of the art, the implementation costs, as well as the nature, scope, the context and purposes of the processing and the varying likelihood and severity of risks to rights and freedoms of individuals, the controller and the processor shall take appropriate technical and organizational measures to ensure a level of security appropriate to the risk safeguards, which include, where appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to maintain confidentiality, integrity, availability and resilience on an ongoing basis of the processing systems and services;

(c) the ability, in the event of a physical or technical incident, to control the availability of and access to the restore personal data in a timely manner;

d) a procedure for testing, assessing and evaluating effectiveness at regular intervals of the technical and organizational measures to secure the processing.

2. In assessing the appropriate level of security, particular account shall be taken of the processing risks, especially as a result of the destruction, loss, alteration or unauthorized provision of, or unauthorized access to, transmitted, stored or otherwise processed data, either accidentally or illegally.

3. Joining an approved code of conduct as referred to in Article 40 or an approved certification mechanism referred to in Article 42 can be used as an element to demonstrate that that the requirements referred to in paragraph 1 of this Article are complied with.

4. The controller and the processor shall take measures to ensure that any

natural person acting under the authority of the controller or of the processor

and has access to personal data, this only on behalf of the controller

processed, unless he is obliged to do so under Union or Member State law.

Date

January 15, 2020

Our reference

z2019-17017

Article 58 Powers

1. Each supervisory authority shall have all of the following investigative powers to:

a) the controller, the processor and, where applicable, the representative of the

to instruct the controller or processor to carry out its tasks

provide required information;

b) conduct investigations in the form of data protection checks;

(c) carry out a review of the certifications issued in accordance with Article 42(7);

d) notify the controller or processor of any alleged breach of this

regulation;

e) obtain from the controller and processor access to all personal data

and all information necessary for the performance of its duties; and

f) gain access to all premises of the controller and processor,

including to all data processing equipment and means, in accordance with

with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following powers to take corrective

measures:

a) warn the controller or processor that with the intended processing operations

likely to infringe any provisions of this Regulation;

b) reprimand the controller or processor where processing infringes

provisions of this Regulation has been made;

(c) the controller or processor instructs the data subject's requests to

exercise its rights under this Regulation;

d) instruct the controller or processor, where appropriate, in a specified manner

and within a specified period, to bring processing operations in accordance with the provisions

of this Regulation;

e) the controller directs a personal data breach to the

to notify the person concerned;

f) impose a temporary or permanent restriction on processing, including a processing ban;

g) rectification or erasure of personal data or restriction of processing under the

Articles 16, 17 and 18, as well as the notification of such acts to recipients to

who the personal data has been provided to, in accordance with Article 17(2) and Article 19;

(h) withdraw a certification or order the certification body to issue a certification pursuant to Articles 42 and 43

revoke certification issued, or instruct the certification body not to issue certification

if the certification requirements are no longer met;

(i) as the circumstances of each case, in addition to or in lieu of the measures referred to in this paragraph,

impose an administrative fine under Article 83; and

j) the suspension of data flows to a recipient in a third country or to an international

order organisation.

3. Each supervisory authority shall have all authorization and advisory powers to:

a) provide the controller with advice in accordance with the procedure of

prior consultation of Article 36;

(b) on its own initiative or upon request, to the national parliament, to the government of the Member State, or

in accordance with Member State law to other institutions and bodies as well as to the public

to provide advice on matters related to the protection of

personal data;

(c) to consent to processing as referred to in Article 36(5), if that prior

consent is required by Member State law;

(d) to advise and approve the in accordance with Article 40(5)

design codes of conduct;

(e) accredit certification bodies in accordance with Article 43;

(f) issue certifications and approve certification criteria in accordance with Article 42(5);

(g) the standard clauses on . referred to in Article 28(8) and Article 46(2)(d).

to adopt data protection;

(h) authorize the contractual terms referred to in point (a) of Article 46(3);

(i) authorize the administrative arrangements referred to in Article 46(3)(b);

j) to approve binding corporate rules in accordance with Article 47.

4. The exercise of the powers conferred on the supervisory under this Article

authority, appropriate safeguards apply, including effective

remedy for justice and due process, as enshrined in the Charter in accordance with the Charter

Union law and Member State law.

5. Each Member State shall provide by law that its supervisory authority is competent for infringements of these

Regulation to the judicial authorities and, where appropriate, an

bring or otherwise take legal action in order to enforce the provisions of this

to comply with the regulation.

6. Each Member State may provide by law that its supervisory authority, in addition to the . referred to in paragraphs 1, 2 and 3 powers has additional powers. The exercise of those powers is without prejudice to the effective functioning of Chapter VII.

Article 83 General conditions for the imposition of administrative fines

1. Each supervisory authority shall ensure that the administrative fines imposed under this Article shall be imposed for the infringements of this Regulation referred to in paragraphs 4, 5 and 6 in any case effective, proportionate and dissuasive.

2. Administrative fines are imposed according to the circumstances of the individual case in addition to or instead of the measures referred to in Article 58(2)(a) to (h) and (j). Bee the decision on whether to impose an administrative fine and on the amount thereof the following shall be duly taken into account in each specific case:

(a) the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the infringement processing in question as well as the number of data subjects affected and the extent of the damage suffered by them injury;

b) the intentional or negligent nature of the infringement;

c) the measures taken by the controller or processor to limit the damage suffered by those involved;

d) the extent to which the controller or processor is responsible in view of the technical and organizational measures that he has implemented in accordance with Articles 25 and 32;

e) previous relevant breaches by the controller or processor;

f) the extent to which there has been cooperation with the supervisory authority to remedy the breach and the limit possible negative consequences thereof;

g) the categories of personal data to which the breach relates;

(h) the manner in which the supervisory authority became aware of the infringement, in particular whether, and if so, to what extent, the controller or processor has notified the breach;

(i) compliance with the measures referred to in Article 58(2), to the extent that they previously apply to the controller or the processor in question with regard to the same matter

are taken;

j) adherence to approved codes of conduct in accordance with Article 40 or approved

certification mechanisms in accordance with Article 42; and

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as

financial gains made, or losses avoided, arising directly or indirectly from the infringement

result.

3. Where a controller or a processor intentionally or negligently engages

relating to the same or related processing activities infringes

several provisions of this Regulation, the total fine shall not exceed that for the most severe

infringement.

4. Infringements of the following provisions shall be subject to administrative in accordance with paragraph 2

fines up to EUR 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:

(a) the obligations of the controller and the processor in accordance with Articles 8,

11, 25 through 39, and 42 and 43;

(b) the obligations of the certification body in accordance with Articles 42 and 43;

(c) the obligations of the supervisory body in accordance with Article 41(4).

5. Infringements of the following provisions shall be subject to administrative in accordance with paragraph 2

fines up to EUR 20 000 000 or, for a company, up to 4 % of the total worldwide annual turnover in

the previous financial year, if this figure is higher:

Date

January 15, 2020

Our reference

z2019-17017

a) the basic principles of processing, including the conditions for consent,

in accordance with Articles 5, 6, 7 and 9;

(b) the rights of data subjects in accordance with Articles 12 to 22;

c) transfers of personal data to a recipient in a third country or an international

organization in accordance with Articles 44 to 49;

(d) all obligations under any law established by Member States under Chapter IX;

e) non-compliance with an order or a temporary or permanent restriction on processing or a suspension of

data flows by the supervisory authority in accordance with Article 58(2) or non-provision

of access in violation of Article 58(1).

6. Failure to comply with an order of the supervisory authority referred to in Article 58(2) is

subject to administrative fines up to EUR 20 000 000 in accordance with paragraph 2 of this Article or,

for a company, up to 4% of the total worldwide annual turnover in the previous financial year, if

figure is higher.

7. Without prejudice to the powers to take corrective action of the

supervisory authorities in accordance with Article 58(2), each Member State may adopt rules

on whether and to what extent administrative fines may be imposed on those

public authorities and public bodies established in a Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be

subject to appropriate procedural safeguards in accordance with Union and Member State law

law, including an effective remedy and due process of law.

9. Where the legal system of the Member State does not provide for administrative fines, this Article

be applied in such a way that fines are initiated by the competent supervisory authority

and imposed by competent national courts, ensuring that these remedies

be effective and have the same effect as those imposed by supervisory authorities

administrative fines. In any case, the fines are effective, proportionate and dissuasive. That

Member States shall notify the Commission by 25 May 2018 of the legislative provisions they have adopted pursuant to

adopt this paragraph and without delay any subsequent amendments thereto and all matters affecting it

amending legislation.

UAVG

Article 14 Duties and powers

1. The Dutch Data Protection Authority is authorized to perform the tasks and exercise the powers

that have been allocated to the supervisory authority by or pursuant to the Regulation.

2. On the preparation of a decision on the approval of a code of conduct, or the amendment or

extension thereof, as referred to in Article 40, fifth paragraph, of the Regulation is Section 3.4 of the General

administrative law applicable.

Date

January 15, 2020

Our reference

z2019-17017

3. The Dutch Data Protection Authority may, in the event of a violation of the provisions of Article 83(4),

fifth or sixth paragraph, of the bye-law, impose an administrative fine not exceeding the amount specified in these paragraphs

mentioned amounts.

4. Sections 5:4 to 5:10a of the General Administrative Law Act apply mutatis mutandis

to corrective measures as referred to in Article 58, second paragraph, under b to j of the

regulation.

5. Without prejudice to Article 4:15 of the General Administrative Law Act, the Dutch Data Protection Authority may de suspend the period for making a decision insofar as this is necessary in connection with the complying with the obligations resting on the Dutch Data Protection Authority pursuant to Articles 60 to and with 66 of the Regulation. The third and fourth paragraph of Article 4:15 of the General Administrative Law Act apply mutatis mutandis to this suspension.