Registered

[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

authoritypersonal data.nl

Date

January 15, 2020

Our reference

z2019-17017

Contact

[CONFIDENTIAL]

Your letter from

July 29, 2019 (your reference: 232958)

Subject

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

Dear [CONFIDENTIAL]

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

1.

Course of the procedure

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

2. In response to the aforementioned report, the AP has launched an investigation. In that context, on 31

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

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

Haga Hospital responded in writing on February 4, 2019.

4. Subsequently, the AP - taking into account the response of Haga Hospital - has the research report

definitively determined and sent to Haga Hospital 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 decree as well as to paragraph

1.2, p. 4

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

Attachment(s) 1

1

Date

January 15, 2020

Our reference

z2019-17017

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

sent to Haga Hospital under penalty. Haga Hospital has both on that intention

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

viewpoint given.

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

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

Article 32, first paragraph, of the GDPR.

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

against the aforementioned decision and requested a period of 6 weeks for supplementing the grounds.

8. In a letter dated 31 July 2019, the AP gave Haga Hospital the opportunity by 11 September 2019 at the latest

to complete the grounds of objection.

9. By letter and fax dated September 10, 2019, as well as by letter and fax dated October 4, 2019, Haga Hospital its grounds of objection.

10. On October 16, 2019, a hearing took place at the offices of the AP. Of hearing is one report made. This report is appended to this decision.

11. On October 17, 2019, an on-site investigation took place at the offices of Haga Hospital in The Hague to verify whether Haga Hospital has complied with the cease and desist order.

12. In response to what was discussed during the hearing on October 16, 2019, Haga Hospital has letter, fax and e-mail dated 5 November 2019 in further detail her appeal to limited financial capacity substantiated.

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

14. In a letter dated December 5, 2019, the AP asked you whether the aforementioned letter from the AP of December 2, 2019 there is reason for Haga Hospital to withdraw the grounds for objection against the order subject to periodic penalty payments. In

In response to this, you indicated in a letter dated December 13, 2019 that Haga Hospital is not a reason sees its grounds for objection with regard to the order subject to periodic penalty payments withdrawn.

2 Earlier, in a letter dated 22 August 2019, the AP has already concluded that Haga Hospital, when implementing the measures set out in its letter, of 9 August 2019 (reference: 2019/0177/CvdW/PM/rv) the proposed measures are complied with that relates to the control of log files. By letters from Haga Hospital dated 24 and 30 September 2019 (reference: 2018/0109x/CvdW/PM/cb and 2018/0109z/CvdW/JP/rv respectively) Haga Hospital has explained how it has implemented given to the burden.

Date

January 15, 2020

Our reference

2.

Legal framework

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

3.

The primary decision

16. Pursuant to Article 58, paragraph 2, opening words and under d and i, in conjunction with Article 83, paragraph 4, 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
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 on Haga Hospital, the AP has imposed an administrative fine and an order
penalty imposed for violation of Article 32, paragraph 1 of the AVG, read in conjunction with
Article 3, second paragraph, of the Electronic Data Processing by Healthcare Providers Decree and the
determined under 12.4.1 of NEN 7510-2 because the requirement of two-factor authentication has not been met and the
requirement to regularly review the log files.

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

19. Article 32 GDPR is, as follows from Article 2.3 of the Fining Policy Rules 2019, classified in category II.
A fine bandwidth 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
fine.4 The AP then adjusts this further provision to the factors described in Article 7 of the
Fining Policy Rules 2019. This allows the base fine to be increased or decreased.

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

21. In addition to an administrative fine, an order subject to periodic penalty payments has also been imposed on Haga Hospital due to

the same violation. The burden extends to Haga Hospital - within fifteen weeks of the date of the

primary decision - to allow access to its hospital information system exclusively 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 one

maximum amount of € 300,000 in total.

3 Stct. 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 fine adding the bandwidth together and then dividing it by two (cf. art. 2.4 Fining Policy Rules 2019).

Date

January 15, 2020

Our reference

z2019-17017

4.

Grounds of the objection

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

No grounds for maintaining NEN standards

Lack of legal basis for enforcement

23. Haga Hospital believes that the AP has no legal basis to take enforcement action. Otherwise than the AP suggests, neither follows from the GDPR nor from the Processing Additional Provisions 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 Electronic Data Processing by Healthcare Providers Decree

(Begs).

24. The power to set further rules for the processing of

personal data (article 26 Wbp) has lapsed with the introduction of the GDPR. It follows that

the disappearance of the basis of the Begz, namely article 26 Wbp, not (exclusively) with article 15j

Wabvpz could be restored. After all, this does not yet grant the AP authority to

to lay down more detailed rules in a particular sector. The Wabvpz is therefore not an elaboration of the AVG, but

stands on its own, next to the AVG and its predecessor, the Wbp. The AP is not authorized to take enforcement action

due to alleged violation of the NEN standards on the basis of the Begz/Wabvpz. To that end, only the

Authorized Healthcare and Youth Inspectorate.

25. It follows from paragraph 2.4 of the explanatory memorandum to the UAVG that the material standards for

data processing follow directly from the GDPR and should no longer be at national level

captured. The AP can therefore not fill in the open standards in the GDPR with national laws

regulations, by means of NEN standards. Haga Hospital refers to considerations 8, 10 and 13

of the preamble to the GDPR. The GDPR requires an autonomous interpretation from the member states. The AP can

therefore do not impose a fine or order subject to periodic penalty payments on the basis of the (U)GDPR for violation of the

NEN standards.

Violation of the principle of legality

26. HagaZiekenhuis is furthermore 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 specified. From the principle of legality laid down in Article 7 ECHR and Article 5:4, paragraph 2, Awb

follows that the AP could not take enforcement action. A sanction can only be imposed for an at or

conduct prohibited by law. In addition, in view of the lex certa-

principle to be sufficiently clear, foreseeable and knowable. According to Haga Hospital, that is not the case here

case because the content of the open standard in Article 32 (1) GDPR could not be known by a concrete

application in practice. The AP should have clarified this open standard first. The reference of the

AP to a report by the Dutch Data Protection Authority from 2013, the AP cannot benefit because this report is based on the Wbp and the NEN standards.

28. The mere fact that Haga Hospital 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)GDPR. Article 5:4, paragraph 2 Awb requires a legal basis. Internal policy is insufficient.

29. Insofar as it would be allowed to test against the NEN, Haga Hospital argues that the AP has omitted to clarify when 'regular review of log files' is involved.

Haga Hospital explained during the opinion session how the control of the logging within Haga Hospital takes place and has explicitly asked the AP for a concrete interpretation of the standard. That should have been reason for the AP to concretize this standard. The AP's argument paragraph 5.2 of the contested decision, in which it substantiates why it has not given any substance to the standard 'regularly', therefore does not apply because it boils down to the necessity of the size of controls depends on the way in which control takes place. And the AP knew the method of control.

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

31. In its letter of October 4, 2019, Haga Hospital provided additional reasons why it believes that the AVG does not offer any scope for further detailing Article 32 AVG by means of NEN standards. She refers in accordance with the jurisprudence of the Court of Justice of the EC from which it follows that Member States do not may add substantive rules or binding interpretation provisions to a regulation.5 The AP does this according to Haga Hospital 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 it

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 periodic penalty payment

Haga Hospital has not been negligent

32. Haga Hospital claims not to have been negligent. In this regard, she points to the following affected

measures:

o An extra warning appears when an employee opens a file;

o There is a mandatory e-learning course for all employees who have access to it

electronic patient record;

o All employees are made aware of professional secrecy and the

importance of confidentiality of patient data;

o Additional information is provided at the introduction 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, Haga Hospital refers to the judgment of the CJEU of 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 protect their patient data additionally;

o Where possible, authorizations will be tightened;

o We are working on a customized solution for checking the logging.7

33. Haga Hospital also indicates that the conclusion that it was negligent is not correct because the AP

goes beyond the fact that implementing two-factor authentication is not a measure that prevents unauthorized access in patient files by employees. After logging in with two-factor authentication is after all, it is still possible for employees to view a patient file without authorization.

34. HagaZiekenhuis also notes that the AP's statement that the hospitals affected by HagaZiekenhuis measures do not relate to 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 context, Haga Hospital also notes that it is contrary to the principles of proper governance in general and the principle of legal certainty in particular to collect an administrative fine on the basis of an unclear standard (the NEN standard with regard to logging is open) and that standard has not been specified by the governing body.

AP has wrongly fined Haga Hospital twice

35. The DPA has imposed a basic fine of € 310,000 on Haga Hospital. This basic fine is by the AP subsequently increased twice by an amount of € 75,000 because, according to the AP, there is "a structural violation that still persists". The AP's substantiation for the former increase of the basic fine amounts to the same as the substantiation for the second increase. The After all, the continuous violation established by the AP is 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 Fining Policy and it is also not reasonable to pay the base fine twice increase due to the same fact. The double increase is therefore also contrary to the ne bis in idem principle. principle (Article 5:43 Awb).

Fine wrongly not reduced

36. Article 7, preamble and under c, of the Fining Policy Rules gives the AP the option to set the basic fine lower if measures have been taken by the controller to reduce the mitigate the damage suffered by those involved. In this context, Haga Hospital refers 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 healthcare and innovate, on the basis of which Hagaziekenhuis remains able to provide sustainable healthcare

7 This custom solution (a software application specially developed for Haga Hospital called [CONFIDENTIAL]) is

implemented and active. Please refer to the letter from Haga Hospital dated September 24, 2019 (reference:

2018/0109x/CvdW/PM/cb) as well as to the letter from the AP dated 2 December 2019 containing the findings in response to

the

on-site investigation on October 17, 2019 to verify compliance with the burden.

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

is.

38. HagaZiekenhuis finally appeals to reduced financial capacity and requests this

reason for punishment. In this regard, Haga Hospital points out in its letter of 5 November 2019

report from accounting firm [CONFIDENTIAL] and a report from the financial strategic

consultancy [CONFIDENTIAL], and further refers to the financial figures of Haga Hospital

about 2019.

Penalty sum set too high

39. The DPA has attached a penalty of € 100,000 to the order for every two weeks that is not (fully)

the burden has been met, up to a maximum amount of € 300,000 in total. Haga Hospital is committed to it

position that these amounts are disproportionate to the alleged conduct. That concludes the decision

conflicts 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 periodic penalty payments is at the expense of the opportunity to invest in healthcare and to innovate. That cannot be the purpose of enforcement. Haga Hospital also believes that a reduction of the periodic penalty payment is justified.

41. The amount of the periodic penalty payment is contrary to the principle of equality. The AP has since the entry into force of the GDPR, various orders subject to periodic penalty payments have been imposed. The penalty that on Haga Hospital is by far the highest.

42. The periodic penalty payment is contrary to the principle of proportionality, because one penalty amount is attached to a load consisting 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.

Judge AP

43. Haga Hospital processes data in its hospital information system electronically and on a large scale (medical) personal data. This (often) involves extremely sensitive health data. This qualify data as a special category of personal data within the meaning of Article 9, paragraph 1, GDPR for which, in principle, a processing prohibition applies unless there is an exception as stated in the AVG and UAVG. It is very important for patients to have confidence in a healthcare provider this personal data is handled with the utmost care and that it is adequately secured. Hospital patients - who are often in a vulnerable position - must always be able to access it trust that their personal data will be treated confidentially and that this will be prevented employees who have no treatment relationship with the patient or who do not need data for the management of care provision or treatment, unauthorized patient files can consult. Against this background, the AP conducted research at Haga Hospital. In response to of the results of that study, it has been established in the primary decision that Haga Hospital none, then

Date

January 15, 2020

has not taken sufficient appropriate technical and organizational measures as referred to in

Article 32, first paragraph, of the AVG and an administrative fine and an order subject to periodic penalty payments have been

imposed. In

The present decision on the objection is made by the AP in response to the arguments you have put forward

grounds of objection do not lead to a different conclusion.

Appropriate measures; two-factor authentication and logging control

44. The violation of Article 32, paragraph 1, GDPR comprises two aspects. The first concerns non-compliance

the requirement of two-factor authentication. It has been found that for users of the

hospital information system was possible to access the data in the digital

patient records with 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 factors

login authentication. As a result, Haga Hospital did not correctly meet the two-factor requirement

implemented authentication in its business operations.9 This has also been recognized by Haga Hospital.10

45. The second reason why Article 32, paragraph 1, GDPR has been violated, is related to not regularly

checking the logging of access to patient files. Logging means that a

care institution structurally keeps track of who has consulted which patient file and when, so that

unauthorized access can be detected and measures can be taken if necessary. It

policy of Haga Hospital provided for a check on the logging of a random sample every year

six patient files.11 In the relevant period covered by the AP's investigation - January 2018 to

October 2018 - there has been one proactive check for unauthorized access12 and 6 checks for

request from patients and staff.13 14

46. One audit in the period from January 2018 to October 2018, compared to the number

patient visits 15 that Haga Hospital receives annually and in 2017 (rounded) amounted 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 (e.g. a token); or something the user is (a biometric). (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 research report, March 2019

10 See 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 from Haga Hospital, 23 October 2018 (reference: 2018/0109c/RdF/PM/rv), answer to question 5 and Annex 3: Authorization Digital Patient Files. 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 from Haga Hospital, October 23, 2018 (reference: 2018/0109c/RdF/PM/rv), answer to question 5.

14 At present, the number of samples is 132 per year. For further details, see the report of findings dated 2 December 2019 as a result of the on-site investigation into compliance with the order subject to periodic penalty payments on 17 October 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 letter from Haga Hospital dated 9 August 2019 (reference: 2019/0177/CvdW/PM/rv). The AP also refers to the figures from the annual report submitted by Haga Hospital for the opinion hearing.

This concerns a total of (rounded off) 381,500 patient visits in 2017, which are divided into 28,500 admissions, 158,000 first outpatient visits, 52,000 first aid consultations and 143,000 nursing days.

number of employees who have (potential) access to patient files17, in the opinion of the AP
not be regarded as 'regular' control and therefore not as an appropriate measure in the sense
of Article 32, first paragraph, of the GDPR. In addition, the AP notes that in that period the Haga Hospital
reactive checks carried out neither independently nor in combination with the proactive check of
the patient file of the well-known Dutchman - can be regarded as a regular check-up.
After all, such reactive checks are solely dependent on an (explicit) request from one
patient or employee.18

47. Also the six (proactive) checks on the logging that Haga Hospital announced19 and carried out20
in 2019, the AP finds, again compared to the number of patient visits - which always result in
consultation of a patient file21 - and the number of employees, insufficient to be regarded as 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
for a continuation of the way under the old regime of Directive 95/46/EC and the Wbp
what was regarded as 'appropriate measures' was implemented and was 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 AP is of the opinion that this explanation also applies under the GDPR
correct interpretation of the standard 'appropriate measures' from Article 32, first paragraph, GDPR. Because
Haga Hospital has not acted in accordance with this explanation, the AP believes that an enforcement order should be
imposed
measures appropriate. After this, the AP will present its position against the background of the objections of
Haga Hospital further motivation.

6.

Review

49. Pursuant to Article 7:11 of the Awb, the AP assesses on the basis of your objection whether it is involved in the primary

decision

rightly so that the order subject to periodic penalty payments and an administrative fine has been imposed.

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

Haga Hospital.

18 The AP notes in this context that the check performed by Haga Hospital is also not in accordance with its own

authorization policy.

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

December 2018, Appendix 3, pages 4-5 and Haga Hospital Response dated October 23, 2018, Appendix 19: Sample Logging

Procedure and

Planning Sample Logging.

20 Report opinion session. P.2, which report is appended to the letter from the AP dated 16 May 2019

(reference:z2019-07604).

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

down to 0.0016%.

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

healthcare institutions-careless-with-medical-data

23 Cf.:

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

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

-

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

Date

January 15, 2020

Our reference

z2019-17017

Jurisdiction, Article 32 GDPR and lex certa

Authority

50. Haga Hospital states that the AP can only impose a fine and an order subject to periodic penalty payments based on the AVG and the UAVG and not on the basis of the Wabvpz and the based on it Begz, with the NEN standards included therein.

51. In this regard, the DPA notes the following. It has been determined in the primary decision that Haga Hospital de (security) standard as laid down in Article 32, first paragraph, GDPR has been violated because insufficient appropriate technical and organizational measures have been taken to ensure a risk-based approach level of security for the processing of personal data. So it's that standard Article 32, paragraph 1, of the GDPR, which the AP has found to have been violated by Haga Hospital.24 Although the primary decision considers that Article 32 of the GDPR in connection should be read with Article 3, second paragraph, of the Begz and the provisions under 12.4.1 of NEN 7510-2, but it cannot be concluded 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 also not the case. In the present case, however, the NEN 7510-2 contained the requirement of two-factor authentication as well as the requirement to regularly update log files assess, the concrete implementation/interpretation of what is in this case 'appropriate technical and organizational measures' within the meaning of Article 32, paragraph 1, GDPR apply. The AP has the fine and the order subject to periodic penalty payments are therefore also not imposed on the basis of and because of a violation of the Wabvpz and/or the Begz and the NEN standards contained therein, but on the basis of not taking appropriate technical and organizational measures within the meaning of Article 32, paragraph 1, GDPR.

52. In its notice of objection, supplemented by letter of 4 October 2019, Haga Hospital also points to European jurisprudence26 This jurisprudence essentially pertains to the prohibition of further to set (binding) rules in national regulations in case a European regulation applies. A however, such a situation does not arise in the present case. No further rules have been set. That doesn't take away

that in a specific case Article 32 GDPR must be applied and interpreted. The application and

interpretation is - in view of the task assigned to it in Article 6, paragraph 3, UAVG to supervise

compliance with the GDPR - to the AP. That is what the AP has done and what it is obliged to do.

It is ultimately up to the national court and the Court of Justice of the EU to assess whether the AP has the

24 Pursuant to 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 AVG and Article 14, third paragraph, of the UAVG, the AP is authorized to impose an administrative fine and an order subject to periodic penalty payments

if there is a violation of article 32, first paragraph, of the AVG.

25 In this context, the AP also notes that Haga Hospital is bound to 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 Haga Hospital states in its appeal, the

authority to set further rules for the processing of personal data for a specific sector (article 26 Wbp) with the

introduction of the GDPR has been canceled, the AP denies. In the opinion of the AP, Article 6, second paragraph and/or third paragraph,

AVG, specifically 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), CJEU 31 January 1978, case 94/77 (Fratelli Zerbone)

Date

January 15, 2020

Our reference

z2019-17017

interpretation given by it of the standards from the AVG is legally correct.27 This means that a

autonomous interpretation guaranteed.

Article 32 GDPR and lex certa

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

54. The lex certa principle requires the legislature, in order to ensure legal certainty, to
describes a norm or prohibited behavior in the clearest possible way.28 Someone must be able to know ter
for what conduct or omissions he may be punished. This requires the implementation of a legal
provision must be sufficiently clear, specific and knowable. However, that doesn't mean it's use
of a vague or open standard is not possible. On the contrary, the legislature can suffice with such
standards. Open norms can be necessary and therefore acceptable because the law must be too
can function under changed circumstances.29 In the so-called Krulsla judgment, the
Supreme Court that when describing crimes, it uses a certain vagueness, consisting in
the use of general terms is sometimes unavoidable in order to avoid behaviors that
be punishable fall outside the scope of the offense description.30 Cannot always be foreseen
how the interests to be protected will be violated in the future and why, if so
provided, otherwise descriptions of offenses would be too refined, resulting in a lack of clarity
disappears and thus harms the importance of the general clarity of the legislation. In addition to the
The Supreme Court also interprets the lex certa principle in this way in the (highest) administrative courts.31

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

56. First of all, according to the text of Article 32(1) GDPR, the measures to be taken must be taken into account
the state of the art, the implementation costs, as well as the nature, size,
context and the processing purposes and the varying likelihood and severity of the risks to the
rights and freedoms of persons. Furthermore, Article 32, first paragraph, opening words, and parts a-d, AVG

made a further specification of what constitutes the 'appropriate technical and organizational measures'

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 in Article 49 of the

Charter of

the fundamental rights of the European Union.

29 ECtHR, Kokkinakis v. Greece, judgment of 25 May 1993, 14307/88.

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

31 See e.g. 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 contains a more specific elaboration of the (general) principle of integrity and confidentiality as

laid down in Article 5, paragraph 1, opening lines and under f, GDPR.

Date

January 15, 2020

Our reference

z2019-17017

a) the pseudonymization 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 to ensure the availability of and access to the

restore personal data in a timely manner;

64. d) 65. a procedure for testing, assessing and evaluating effectiveness at regular intervals

of the technical and organizational measures to secure the processing.

The second paragraph of Article 32 GDPR further stipulates that in the assessment of the appropriate

security level, in particular taking into account the processing risks resulting from
unauthorized access to transmitted, stored or otherwise processed data, either by
accident or wrongful.

57. Thus, Article 32, GDPR, partly in conjunction with the preamble33, already provides a further interpretation of the standard 'appropriate technical and organizational measures' and it is indicated that they are specifically taken into account must be kept. Including ‘guaranteeing integrity’34 and ‘unauthorised access'35. The requirements of two-factor authentication and regular checking of the logging form one further elaboration/interpretation of those concepts. In view of the foregoing, in the opinion of the AP, requiring two-factor authentication and regular auditing of logging under it take appropriate technical and organizational measures to prevent unauthorized access prevent or hinder, therefore reasonably foreseeable. This must be considered that Article 32 GDPR provides a standard that is addressed to all data controllers, regardless of which market segment they are active. The GDPR therefore covers all areas and all forms of cover data processing. All data 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 technology. To be able to implement this in a meaningful way, it is necessary to prescribe it in detail measures are not possible in view of the speed with which technology is currently highly digitized society progresses. With the rapidly developing technology, a new one will therefore be introduced periodically assessment must (be able to) be made. This requires (a certain degree of) flexibility and future-proofing of the standard, and that justifies it – against the background of the above

33 Recital 83 in the preamble to the GDPR is very similar in text to what is stated in Article 32 GDPR: In order to ensure security and prevent the processing from infringing this Regulation, the controller or the processor to 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, with including confidentiality, taking into account the state of the art and the implementation costs against the risks and the nature of the personal data to be protected. When assessing the

data security risks, attention should be paid to risks that arise with

personal data processing, such as the destruction, loss, alteration, unauthorized disclosure of or the

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, opening words, and part b, GDPR.

35 Article 32, second paragraph, GDPR.

cited case law listed under marginal number 52 – in this case there 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 AP to the standard 'appropriate technical and

organizational measures' is sufficiently clear, determined and knowable, is furthermore the following

interest. In general, this applies to the material standards that govern the processing of personal data

must comply with 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 wording 'appropriate technical and

organizational measures' - as included in article 32 AVG - there is a continuation of

which already applied under Directive 95/46/EC and the Wbp.38 There is no question of a material change. below

in those circumstances, it is obvious - also with a view to legal certainty - that in the past

to continue the interpretation followed in the interpretation of Article 32, paragraph 1, GDPR. That means that the already in

past interpretation via the requirements of two-factor authentication contained in the NEN standards

the regular assessment of the log files are maintained.39 The AP is also always clear

propagated 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

remains in healthcare and these guidelines must be followed.40 In a similar sense, the GDPR

Helpdesk for Care, Welfare and Sport communicated this. 41

59. In view of the foregoing, the AP is of the opinion that the European legislator has sufficed with the

standard laid down in Article 32 GDPR regarding the appropriate technical and organizational to be taken

measures.

A closer look at the 'regular inspection' standard

60. Specifically with regard to the requirement of regular checking of the logging and the objection of

Haga Hospital that this standard is too vague, the AP also notes the following. The AP is from

opinion 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 GDPR): (…)"In the

concept <<appropriate>> implies that the security is in accordance with the state of the art. This is initially one

question of professional ethics of persons charged with information security. The standards of these ethics are set out in this provision

provided with a legal capstone, in the sense that a legal obligation is attached to it for the controller. 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. " (…). (emphasis added by the AP). See TK 1997-1998, 25

892, no. 3, p. 98-99.

37 According to recital 9 in the preamble to the GDPR, the objectives and principles of Directive 95/46/EC remain valid.

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

to prevent loss or unlawful processing.

39 For example, it follows from the report 'Access to digital patient records 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/zorgproviders-en-de-avg?qa=nen%207510&scrollto=1 and

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

-

concerns-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.

Date

January 15, 2020

Our reference

z2019-17017

of one file (regarding 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

'regular' can be qualified. 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

number of patients and staff present at the hospital. That generates a very large processing

amounts of data. Haga Hospital has to deal with a large number of patient visits and has a lot

employees who (potentially) all have access to the patient files.46 The 'open'

considering the character of a hospital (everyone can visit a hospital; well-known and

unknown patients), the sensitivity of the personal data and the fact that good care was provided

should prevent access to - and therefore processing of - medical data

may be an impediment, (precisely) this means that a regular check on the logging is proportionate to

the number of files and file consultations is necessary for good security. One (manual)

random sample of 6 patient files does not give evidence of sufficient feeling of this in the opinion of the AP

urgency and does not indicate that Haga Hospital is 'in control' in this area. Haga didn't have one

automatically organized control process, but used a manual control that, moreover, on
was carried out on a very occasional basis. As stated, this method does not fit in well with the large number
patient visits/file consultations and the associated risk of possible unauthorized access
file consultations. In the AP's opinion, therefore, it is not possible to speak of a suitable one
measure. Haga Hospital should also have realized that and should have been clear in view of the standard that the
AP also used before the entry into force of the GDPR. Seen against that background is of a te
vague/unclear standard, as Haga Hospital states, is out of the question.

61. That the AP did not indicate in advance how many files in the case of Haga Hospital
must be assessed, does not mean, as HagaZieknhuis argues, that this means that the standard is too
is vague and violates the principles of legality or legal certainty. How many
dossiers to be assessed depends in part on the facts and circumstances of the case
concrete situation, such as the number of loggings in relation to the number of patient files and the number
employees that can access, and can therefore be different on a case-by-case basis. In addition, the AP notes that it op
quantifying in advance what is 'regular' is often not possible and/or desirable because that is
may undermine the required level of protection in a specific case. This would, also considering
the time-bound nature of the state of the art, the ability to respond in a timely manner
changed circumstances and future developments, the application of the regulations in high
degree can hinder. It is therefore not inconceivable that it will become possible in the near future
by means of, for example, specific software applications in a simpler manner and on a larger scale

42 For more information on the factual findings regarding logging, see the AP investigation report of March 2019, p. 13 and 14
with
including references to the relevant sources.

43 For an explanation of this number, see appendix (section 2.1) to the letter from Haga Hospital dated 9 August 2019
(reference:
2019/0177/CvdW/PM/rv).

44 See appendix (section 2.1) to the letter from Haga Hospital 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

Haga Hospital.

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

[CONFIDENTIAL] for the purpose of checking the logging confirms this position.47

More is expected from professional parties

62. Finally, the following is noted in connection with the foregoing - unnecessarily. For a

successful appeals to the lex certa principle are being made more by professional parties, such as Haga Hospital

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

have insight into the meaning of (open) norms addressed to them and, if necessary, show due diligence

information 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 said, qualify as special

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

a ground for exception and care has been taken for extra guarantees. It was on the way

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

of Article 32 AVG 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 Haga Hospital itself was very aware of the measures to be taken on the ground

of Article 32 of the GDPR. The AP deduces this from the assessment made by Haga Hospital itself

its authorization policy, entitled 'Authorization of Digital Patient Files'. Haga Hospital makes this

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

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

7510.49

Conclusion lex certa

64. In view of the above, 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 is unauthorized

access to patient files by employees can be (completely) prevented.

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

set out with reasons - one of the mandatory measures to be taken is appropriate measures within the meaning of Article 32

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

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

control measures, the aim is to prevent unauthorized access to systems and applications as much as possible

47 For more information about this software, see the letter from Haga Hospital 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, par. 3.5 (ECLI:NL:HR:2000:AA7954), HR, judgment 18 January 2005, par. 3.4

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

CBb 18 December 2018, par. 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 of Unlawful Access to Patient Records' of May 2018 (reference: 20180412ISO01).

Date

January 15, 2020

Our reference

prevent.50That this measure, as Haga Hospital states, is not a measure that guarantees that
unauthorized access to patient records by employees no longer occurs, but 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 checking the logging -
does not stand alone, but must be considered in conjunction with all other appropriate considerations to be taken
measures. It is the combination of these measures that enables Haga Hospital to provide the
to manage the protection of personal data as well as possible and to prevent infringements as much as possible
prevent.

International value NEN standards

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

68. With regard to this ground for objection, the AP first notes that - as above under marginal number
52 has already 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 has done so in the primary decision and
in this decision by requiring two-factor authentication and requiring log files to be regularly
judge. This does not mean that (in advance) there is a situation that goes against one
autonomous interpretation of the GDPR. Whether this explanation stands in the way of the uniform application of the GDPR is
possible
if desired, be submitted 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 and
NEN-EN-ISO 27799:2016 (en).51 These standards have been developed in an international context by

ISO (International Organization for Standardization) or IEC (International Electrotechnical Commission). ISO and IEC together form a system of bodies specialized in worldwide normalization. National organizations that are members of ISO or IEC participate in developing International Standards through technical committees established by the appropriate organization for the benefit of standardization in specific technical fields. Technical committees of ISO and IEC work together on topics in which they have a common interest. Others international organisations, both government agencies and NGOs, in cooperation 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 then given the NEN-ISO or NEN-IEC code. Standards with the coding: NEN-EN-ISO are accepted in Europe.52

50 Cf. section 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-internationale-norms.htm

In short, the relevant NEN standard is therefore about standards at international and European level are accepted and used.53

Amount of the fine and periodic penalty payment

69. HagaZiekenhuis puts forward various objections which, in its opinion, should lead to penance moderation. These are discussed below.

Negligent culpability

70. Haga Hospital 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 Hagaziekenhuis 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 The AP Haga Hospital accuses the measures of negligence. To that extent, these measures are therefore independent of the measures taken by HagaZienkenhuis.

72. The AP has motivated why the number of random checks carried out by Haga Hospital is ten for the purpose of checking the logging (evidently) cannot be regarded as 'regular control" and is therefore contrary to Article 32 GDPR. That the AP does not have in advance in that regard indicating how many random samples are sufficient does not mean that, such 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 statement of HagaHospital that manual checking is very time-consuming does not mean that HagaHospital would thus be released from the obligation under Article 32 GDPR and would therefore suffice with a random check of six files. Moreover, with regard to Haga Hospital's statement, the AP points out that it is manual checking is time consuming, on the capabilities of specific software applications that do this in important degree can be overcome. The AP is of the opinion that it would have been on the road from Haga Hospital here show initiative sooner by acting actively and adequately.

Ne bis in idem

73. HagaZiekenhuis further argues that it has wrongly increased the basic fine twice occurred. According to Hagaziekenhuis, the substantiations for these increases are the same down. And that, in the opinion of Haga Hospital, is contrary to the AP's fining policy rules 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 preface” on p. 1 of the document NEN-EN-ISO/IEC 27002:2017).

54 In this context, the AP also refers to what has been considered in marginal number 57.

74. The AP cannot follow HagaZiekenhuis in its argument and considers this as follows. The AP has in the primary decision increases the basic amount of the fine based on two factors. This fine aggravating factors are listed in Article 7, under a and b, of the Fining Policy Rules and are derived from Article 83, second paragraph, under a and b, of the AVG.55

75. The first increase of the basic fine by €75,000 based on the factor 'nature, seriousness and duration of the infringement' (Article 7, under a, of the Fining Policy Rules) is related on the one hand to the nature and seriousness of the violation and, on the other hand, the duration of the violation.

With regard to the nature/severity, it is important that it concerns the lack of two suitable ones (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 data patient file57, 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 who are greatly embarrassed 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 context it is important that the violation existed since in each case January 2018 and had not yet ended at the time of the imposition of the fine on 18 June 2019.

76. The second increase of the basic fine by €75,000 is based on Article 7, preamble and under b, of the

Fining Policies. It is an increase due to the negligence of Haga Hospital. Despite the
management of Haga Hospital was aware of the unauthorized inspection of the file in question,
has she wrongly seen no reason to take timely measures aimed at a correct
implementation of using two-factor authentication and regularly checking the
log files. In that regard, the AP notes that the argument put forward by Haga Hospital from
lack of time is not a legitimate argument to refrain from taking security measures and thus
to allow the violation to continue.59 In the opinion of
the AP the second increase of the basic fine by € 75,000.

77. In conclusion, the DPA notes that the reason for the first increase in the basic fine differs from that one
for the second increase. The increases are based on various factors from the GDPR and the
Fining policy rules that are taken into account when determining the amount of the fine. Of a
there is therefore no question of a double fine and the ne bis in idem principle is therefore not at issue here. It
The objection raised in that context is without merit.

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 option of two-factor
login authentication.

57 According to Haga Hospital's own investigation 'Final Report Investigation of Unlawful Access to Patient Files' of May 2018,
(p. 27
at the top) it concerns 85 employees of HagaHospital who have had unlawful access to the patient file of the
famous Dutchman. See also AP Research Report March 2019, p. 4.

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

59In this context, the DPA refers to the WP 253 Guidelines, which mention as an example of the “negligent nature of the
infringement”:
not applying technical updates in a timely manner (WP 253, 2016/679, p.12).

z2019-17017

Date

January 15, 2020

Penalty mitigation

78. Haga Hospital is of the opinion that there is a fine-reducing circumstance as referred to in
Article 7, preamble and under c, of the Fining 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, preamble and under c, of
the Fining Policy Rules gives the AP the option to reduce the basic fine if the
measures have been taken by the controller to mitigate the damage suffered by the data subjects
to limit. The measures taken by Haga Hospital are aimed at complying with the op
Haga Hospital has an obligation under Article 32, first paragraph, of the AVG, but lead to it
In the opinion of the AP, the damage suffered by the parties concerned is not, or insufficiently, limited. In
in this regard, the AP notes that HagaZiekenhhuis, with regard to the two-factor authentication and the
check on the logging after they have been set by 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 observed violations60
has made insufficient efforts to take sufficient and appropriate measures in a timely manner. The AP then also sees
no reason to mitigate the fine imposed on the basis of Article 7, preamble and under c, of the
Fining Policies.

80. According to Haga Hospital, there is also a reason for reducing the fine 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
at the expense of the ability to invest and innovate. Haga Hospital also has in this regard
expressly invoked reduced capacity and she has stated her position in this regard
substantiated with two reports in which various hospitals, including Haga Hospital, by
[CONFIDENTIAL] and [CONFIDENTIAL] were assessed on their financial health.61

81. The AP also sees no reason to moderate the fine in this regard. When determining the height of the administrative fine must be taken into account pursuant to Section 5:46(2) of the Awb proportionality principle. In this context, the administrative body must take into account, if necessary the circumstances under which the offense was committed. From 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 fine should be moderated.64 De However, the AP does not consider Haga Hospital's financial situation to be such that it should be concluded

60 P. 14-15 of the AP research report, March 2019.

61 These are 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 reduction of the fine due to reduced capacity is indicated. The AP has hereby submitted the annual accounts of 2018 as well as the information provided by Haga Hospital 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 Haga Hospital cannot bear a fine of € 460,000. The return for 2019 is now forecast at € 947,00066 In addition, the annual accounts show that Haga Hospital had access to

€ 24,011,362 in freely available liquid assets.67 68 The circumstance that [CONFIDENTIAL] the
financial health of Haga Hospital - in the context of a benchmark in which the financial
researched the position of Dutch general hospitals - rated it with a 4 (2017)
and a 569 (2018) because its return is below the 2% standard and also below the market average of
1.48%, Haga Hospital cannot benefit either. Although the AP acknowledges that the financial situation of
HagaHospital is worse compared to other hospitals, this does not mean that
Haga Hospital is insufficiently able to pay the fine imposed on it. The AP considers the
argumentation put forward by Haga Hospital in view of the financial resources at its disposal
insufficient to mitigate the fine in view of the ability-to-pay principle. The same goes for
assessment of [CONFIDENTIAL] who has the return and EBITDA70 of Hagaziekenhuis
rated.

84. That the fine is directly at the expense of the (scarce) resources that would otherwise be used for other purposes
could have been used, the AP acknowledges and endorses Haga Hospital's statement
the scarce resources of a hospital should in principle be spent on care. Nevertheless, this is possible
argument Haga Hospital in this case to no avail. The protection of personal data is also important
to 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 fined at all.

Load under duress

Haga Hospital meets the burden

65 In this regard, the AP notes that, pursuant to Article 38 UAVG, the effect of the decision imposing an administrative fine
is suspended until the appeal period 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 from Haga Hospital dated 5 November 2019, p. 2.

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

December 2018, p. 17.

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

indicated that controllers and processors cannot breach 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 for Earnings Before Interest, Taxes, Depreciation and Amortization. It is used as a benchmark for the

profit that a company makes with its operational activities without the costs and revenues of the financing being included

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

Date

January 15, 2020

Our reference

z2019-17017

85. Haga Hospital states that it will maintain its objection to the order subject to periodic penalty payments,

notwithstanding the letter from the AP dated December 2, 2019 in which the AP states that the order has been complied with.

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 about this. 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 suffering from

satisfied. It should be noted that the checking 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."

It is stated in the above quote that it appeared that Haga Hospital complied with the order. 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 checking of the logging should take place - as a result of the duty to take appropriate measures under Article 32 GDPR - is dynamic in nature. That holds due to the time-bound nature of the prior art, and the ability to respond in a timely manner to be able to respond to any changed circumstances and future developments (see also for this marginal number 57). Against that background, Haga Hospital is based on the resting on her obligation pursuant to Article 32 GDPR to continuously monitor the control process and, if necessary, to improve, specifically when it comes to refining the business rules. That depends on the finding that Haga Hospital currently meets the burden. However, what now becomes appropriate considered, this need no longer be the case in the (near) future. It is also for that reason that it is required that controllers go through the PDCA improvement cycle in order to comply with Article 32 AVG and at the time article 13 Wbp - a permanent appropriate security level in the organization guarantees.72 That is what the AP wanted in its letter of 2 December 2019 to Haga Hospital. give, 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 December 2, 2019, the order subject to periodic penalty payments has not been lifted and can re-investigate in the (near) future whether the order is still adhered to. 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 to the alleged conduct. According to Haga Hospital, 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 guidelines are still current and useful in this respect. See: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publishes-guidelines-security-of-personal data

73 Cancellation is only relevant in this case if HagaZiekenhuis makes a request to this effect pursuant to Article 5:34 Awb.

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

88. It is assumed that Haga Hospital has complied with the order and no penalty payments have been forfeited. For this reason, the AP does not see what interest HagaZiekenhis still has in the grounds of objection put forward with regard to the order subject to periodic penalty payments. Separately, the AP notes the following.

89. The amount of the periodic penalty payment must be in reasonable proportion to, on the one hand, the seriousness of the interests violated by the violation of the statutory provision and, on the other hand, the intended effective operation of the penalty. It is important that the periodic penalty payment provides such an incentive must assume that the imposed order will be complied with and forfeiture of the periodic penalty payment will be avoided. The AP is of the opinion that a penalty has been imposed in this case, which is reasonable relationship in the aforementioned sense and considers as follows.

90. With regard to the seriousness of the interest violated by the violation of the statutory provision the AP emphasizes that this concerns extremely sensitive health data. Qualify this data, as noted several times, as a special category of personal data within the meaning of Article 9, first paragraph, GDPR for which a processing prohibition applies in principle, unless there is an exception such as stated in the AVG and UAVG. It is very important for the confidence of patients in a healthcare provider It is important that this personal data is handled with the utmost care and that it is secure in terms of security meet the highest standards. In that context, it should be noted that the issue in this case is the lack of two fundamental security measures and that, despite the fact that the management of Haga Hospital on was aware of the unauthorized inspection of the file in question, wrongly had no reason to do so has seen to take timely measures to ensure proper 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 as stated in the contested
decision have been established.

91. HagaZiekenhuis is of the opinion that the penalty imposed is contrary to the principle of equality and
points to earlier orders imposed by the DPA in which lower penalty payments have been set. This
In the AP's opinion, the ground for objection does not serve any purpose and explains that position as follows.

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

93. With regard to the penalty payments imposed on other healthcare providers in 200974, and to which
Haga Hospital with an appeal to the principle of equality, the AP notes that cases
concerned from a relatively distant past (now ten years ago) - they took place in another

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

zeitgeist and pre-dating the GDPR - and involving violations of a distinctly different
earth. It concerned failure to comply with obligations of a (mainly) administrative nature, such as
not carrying out a risk analysis, not drawing up a risk analysis report
information security or an information security officer job profile, it is not
appointing/appointing an information security officer and a portfolio holder
information security. In the case of Haga Hospital, there are two fundamental security measures

- two-factor authentication and regular logging - which have not been applied. Moreover, in case of
Haga Hospital a serious security incident in advance, with which the context is also clearly different
used to be. It is also important to note in this context that the CBP - the predecessor of the AP - has already
earlier in 2013, after research at various healthcare institutions, it was found that no provision was made
sufficiently appropriate measures with regard to access to patient files (treatment relationship) and ten
with regard to checking the logging.75

94. When it comes to the penalty in the case of the National Police, and where Haga Hospital points out
that in that case it was a penalty of € 50,000 every two weeks, the AP notes that in that case it
one violation and not two as in the present case. This circumstance makes all the difference
the imposed penalty payments are explicable in the opinion of the AP. In addition, the maximum amount
of € 320,000 in 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 above and to illustrate the case-specific nature of the amount of a
The DPA also points out the order subject to a penalty imposed on VGZ in 2018. The height of the
Penalty payment there amounted to € 150,000 per week and with a maximum of € 750,000, due to a fact that
VGZ employees actually had access to personal data concerning health while
that was not necessary for their work (without it being established that this
employees actually consulted this data).76 It follows that the AP also higher
imposes penalty payments in a case that is comparable in important respects to the present order under
penalty.

96. According to HagaZiekenhuis, the imposed penalty payment is also in conflict with the principle of proportionality
because one penalty amount is linked to an order that consists of two parts, which also means that
penalty payments are forfeited if the first part of the order is, but the second part of
the load is not executed. The AP cannot follow Haga Hospital's point of view and notices it
next on.

97. In itself there is no obligation to impose the order subject to periodic penalty payments on the proposed by Haga Hospital

way, and according to the AP there is no reason to do so in this case. The aan Haga Hospital

The 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

Date

January 15, 2020

Our reference

z2019-17017

obligations must be fulfilled in order to ensure compliance with Article 232 GDPR. It

involves a cumulation of measures that together ensure that, in accordance with Article 32

AVG is acted upon. Even if one of these obligations is not met, it is still

there is a violation of Article 32 GDPR. The point is to achieve simultaneity

complied with all obligations arising from the duty to take appropriate measures.

98. Haga Hospital finally points to the enormous challenge of Haga Hospital to be financially sound

and argues that the penalty order is at the expense of the ability to invest and to

innovation in healthcare. According to Haga Hospital, that cannot be the intention of enforcement and that

justifies, according to Haga Hospital, a reduction of the penalty. The AP follows the argument of

Haga Hospital is not and is considering the following.

99. The order subject to periodic penalty payments must provide such an incentive that the imposed order is carried out

without a penalty being forfeited.77 This point of view does not relate to the determination of

the periodic penalty payment takes into account the fact that the periodic penalty payments are forfeited

at the expense of the opportunity to invest and innovate in healthcare, because then the incentive to

burden to carry out too much is removed. In this context, the AP draws a comparison with the ruling

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 means, does not provide the offender with sufficient incentive to load to end. It also follows from previous case law that the financial circumstances of the in principle, the offender is not allowed to play a role in determining the amount of the penalty.79 De AP also considers the grounds of objection put forward by HagaZiekenhuis in this context as an appeal 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 Section 7:11(1) of the General Administrative Law Act, the AP contested it decision reconsidered in response to the objections raised. In this review, the AP assesses whether it has rightly decided to impose a fine and an order subject to periodic penalty payments.

101.

In view of the foregoing, the AP is of the opinion that it is justified in taking the primary decision until the imposition of the fine and order subject to periodic penalty payments has been made. Nor is there one change of relevant facts and circumstances since the primary decision, so that there is no reason to revoke the primary decision and to take a different decision.

77 See e.g. 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

Operative part

7.

The Dutch Data Protection Authority declares the objection unfounded.

Yours faithfully,

Authority for Personal Data,

Mr. A. Wolfsen

Chair

Remedies Clause

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

decision pursuant to the General Administrative Law Act to file a notice of appeal with the court (sector

administrative law) in the district in which you live. 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 rightly decided to reject your AVG complaint in the primary decision. The reconsideration takes place (in principle) with due observance of all facts and circumstances as they exist at the time of the review.

AVG

Article 32 Security of processing

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

a) the pseudonymization 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 to ensure 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 unlawfully.

3. Adhering to 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 met.

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

natural person acting under the authority of the controller or processor

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

processed, unless he is required to do so by 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

controller or processor for the performance of its tasks

provide required information;

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

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

d) notify the controller or processor of an alleged breach of these

regulation;

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

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

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

including all data processing equipment and means, in accordance

with Union or Member State procedural law.

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

measures:

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

probable infringement of provisions of this Regulation;

b) reprimand the controller or the processor when processing operations infringe

provisions of this Regulation has been made;

c) the controller or the processor shall order the data subject's requests

to grant the exercise of its rights under this Regulation;

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

and within a specified period, to bring processing operations into line with the provisions

of this regulation;

e) order the controller to commit a personal data breach to the

inform the data subject;

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

g) rectify or erase personal data or restrict processing pursuant to the

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

to whom the personal data have been disclosed, in accordance with Article 17(2) and Article 19;

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

withdraw any certification issued, or order the certification body not to issue a certification

if the certification requirements are no longer met;

i) depending on the circumstances of each case, in addition to or instead of the measures referred to in this paragraph,

impose an administrative fine under section 83; and

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

order organization.

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

a) advise the controller 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

provide advice on matters related to the protection of

personal data;

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

consent is required by Member State law;

(d) to issue an opinion on 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 referred to in Article 28(8) and Article 46(2)(d) on

adopt data protection;

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

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

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

4. On the exercise of the powers conferred on the supervisory authority under this article

authority, appropriate safeguards, including effective ones, shall apply

provision of 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 to enforce these

Regulation to the judicial authorities and, where appropriate, against it

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

regulation to comply with.

6. Each Member State may provide by law that its supervisory authority, in addition to the

powers has additional powers. The exercise of those powers is without prejudice

to the effective operation of Chapter VII.

Article 83 General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that administrative fines imposed under this

Article be imposed for the infringements of this Regulation referred to in paragraphs 4, 5 and 6 in each case

be effective, proportionate and dissuasive.

2. Administrative fines shall be imposed according to the circumstances of the specific case

in addition to or instead of the measures referred to in points (a) to (h) and (j) of Article 58(2). Bee

the decision on whether an administrative fine will be imposed and on its amount

the following shall be duly taken into account for each specific case:

a) the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the

processing in question as well as the number of data subjects affected and the extent of the harm suffered by them

injury;

b) the intentional or negligent nature of the breach;

c) the measures taken by the controller or processor to

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 it has implemented in accordance with Articles 25

and 32;

e) previous relevant breaches by the controller or processor;

f) the degree of cooperation with the supervisory authority to remedy the breach and the

limit possible negative consequences thereof;

g) the categories of personal data affected by the breach;

h) the way in which the supervisory authority became aware of the breach, 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), insofar as they have previously been applied to the

controller or the processor concerned in relation 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, which may or may not result directly from the breach

result.

3. If a controller or a processor intentionally or negligently with

in relation to the same or related processing activities infringes

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

infringement.

4. Breaches of the provisions below shall be subject to administrative action in accordance with paragraph 2

fines of up to EUR 10 000 000 or, for a company, up to 2% of its total annual worldwide turnover in

the previous financial year, if this figure is higher:

a) the obligations of the controller and the processor in accordance with Article 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 organ in accordance with Article 41(4).

5. Breaches of the provisions below shall be subject to administrative action in accordance with paragraph 2

fines of up to EUR 20 000 000 or, for a company, up to 4% of its total annual worldwide 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) the transfer of personal data to a recipient in a third country or an international one

organization in accordance with Articles 44 to 49;

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

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

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

of access contrary to Article 58(1).

6. Non-compliance with an order of the supervisory authority referred to in Article 58(2) is

subject to administrative fines of 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 this

figure is higher.

7. Without prejudice to the corrective action powers of the

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

regarding the question whether and to what extent administrative fines can 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 is

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

law, including effective remedy and fair administration of justice.

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 legal remedies

be effective and have an effect equivalent to those imposed by supervisory authorities

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

Member States shall communicate to the Commission, by 25 May 2018 at the latest, the legislative provisions they adopt

pursuant to

adopt this paragraph, as well as without delay any subsequent amendments thereto and any affecting thereto

amending legislation.

UAVG

Article 14 Tasks and powers

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

assigned to the supervisory authority by or pursuant to the Regulation.

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

an extension thereof, as referred to in Article 40, paragraph 5, of the Regulation is Section 3.4 of the General

administrative law applies.

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, fourth,

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

amounts mentioned.

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, parts b to j of the

regulation.

5. Without prejudice to Section 4:15 of the General Administrative Law Act, the Dutch Data Protection Authority may authorize the

suspend the period for issuing a decision insofar as this is necessary in connection with the

compliance with the obligations of 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.