Confidential/Registered

[CONFIDENTIAL]

Date

February 4, 2021

Our reference

[confidential]

Contact

[confidential]

Subject

Decision to impose an administrative fine

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authoritypersonal data.nl

Dear [data subject],

The Dutch Data Protection Authority (hereinafter: AP) has decided to impose an administrative fine of € 12,000.00 on you.

to impose. The AP is of the opinion that, in any case, in the period from July 1, 2018 to May 29, 2019, you

has not complied with your obligation to use appropriate technical

and organizational measures (Article 32, paragraph 1, of the General Regulation

data protection; hereinafter: GDPR).

The decision is explained below. Section 1 contains an introduction. Section 2 discusses the

processing, processing responsibility and the observed violation. In paragraph 3

discussed the authority of the AP to impose a fine, and the amount of the fine. Section 4

finally contains the decision (operative part) and the legal remedies clause.

Introduction

1.

1.1. About the offender

The company “[company]” is driven by [data subject]. On the website of the

orthodontic practice it is stated that the practice has eleven employees in addition to [person concerned] as an orthodontist.

The practice is located at [address] and the company is registered in the trade register of the

Chamber of Commerce under number [Chamber of Commerce number].

1

Date

February 4, 2021

Our reference

[confidential]

1.2.

2.

2.1.

Background to the investigation and process

On November 27, 2018, the AP received a complaint as referred to in Article 77 of the GDPR. According to the

complaint, sensitive data is processed via the registration form on the website of the orthodontic practice

requested, such as the citizen service number (hereinafter: BSN), but the data will then be

sent unencrypted.

On February 26, 2019, the AP visited the website of the orthodontics practice and took screenshots thereof

made.

In a letter dated 29 May 2019, the AP requested information from [person concerned]. [Involved person] has access to that

letter of 4 June 2019 responded to.

On July 4, 2019, the AP again visited the website of the orthodontics practice and took screenshots thereof

made.

In a letter dated 12 August 2019, the AP asked [person concerned] for further information. [Involved person]

responded to this by letter dated 19 August 2019.

The findings and conclusions of the investigation are set out in a report dated August 27, 2019.

By letter of 12 September 2019, the AP sent the investigation report to [person concerned]. The AP has thereby expressed the intention to impose an administrative fine and [person concerned] in the given the opportunity to comment on it.

By letter of 7 October 2019, supplemented by that of 9 and 12 December 2019, [person concerned] has submission submitted.

Facts and Review

The relevant laws and regulations are listed in the appendix to this decree.

Processing of personal data

At the time of the complaint, the website of the orthodontic practice contained a form for registration of new patients. This form contained fields for, among other things, name and address details, date of birth, BSN, telephone numbers of the patient and the parents, information about the school, general practitioner, dentist and the insurance company. This data concerns information about an identified or identifiable natural person, and are therefore personal data as referred to in Article 4, opening lines and under 1 of the GDPR.



Date

February 4, 2021

Our reference

[confidential]

It follows from the letter from [person concerned] dated 19 August 2019 that after sending the form, the data entered were stored online. The orthodontics practice received a notification by e-mail of the new registration. An employee of the practice logged in to the website, opened the data of the registration and created a new patient in its own patient file. Then were the data stored online has been deleted, according to [person concerned]. This set of processing, but also

every part thereof, including the recording, storage and destruction of data, is a

processing of personal data as referred to in Article 4, preamble and under 2, of the GDPR.

Controller

[Data subject] determines the purpose and means of the processing of personal data. It

after all, the registration form serves to obtain data from new patients of her

orthodontic practice run as a sole proprietorship, necessary for the treatment and the financial

handling thereof. [Data subject] is thus the controller, referred to in Article 4, opening words

and under 7 of the GDPR.

2.2.

2.3. Violation regarding the security of processing

2.3.1. Introduction

Pursuant to Article 32(1) of the GDPR, the controller is obliged to

to take appropriate technical and organizational measures to control the processing of personal data

to protect against, among other things, loss or unlawful processing of the data. These measures

must guarantee an appropriate level of security, taking into account the state of the art and

the implementation costs, the risks of the processing and the nature of the data to be protected.

The question whether the controller has the data specified in Article 32, paragraph 1, of the GDPR

has taken measures, in cases such as the present one is assessed as follows. The processing

of a patient's BSN by a healthcare provider must comply with NEN 7510. That is a

healthcare information security standard. The obligation to comply with that standard follows

from article 2 of the Regulation on the use of citizen service numbers in healthcare, read in conjunction with article 8

of the Additional Provisions for the Processing of Personal Data in Healthcare.1 Also outside these statutory provisions

obligation with regard to the BSN, NEN 7510 is the general for healthcare

contains accepted security standards.2 NEN 7510 is further elaborated in NEN 7510-1 and

NEN 7510-2.

Chapter 10 of NEN 7510-2 discusses control measures with regard to cryptography.

These measures aim to ensure the correct and effective use of cryptography to

1 Article 8, paragraph 1, of this Act relates to the provision of care. It follows from Article 1, preamble and under b, of that Act that the

financial-administrative settlement is also part of this. The settlement starts with the delivery of the required information data, such as the citizen service number. Compare the development history of this provision (Parliamentary Papers II 2005/06, 30 380, no. 3, p. 20).

2 Compare the Dutch DPA Guidelines for the Protection of Personal Data (Stcrt. 2013 no. 5174, p. 11).



protect confidentiality, authenticity and/or integrity of information. In section 10.1.1 state that to protect information a policy for the use of cryptographic control measures should be developed and implemented. These can include are used for the purpose of ensuring confidentiality, by encrypting information use to protect sensitive or essential information, during storage or transmission.

Chapter 13 of NEN 7510-2 discusses control measures with regard to communication security. Section 13.2 contains control measures related to information transport. The purpose of these control measures is to maintain the security of information that is exchanged within an organization and with an external entity. In section 13.2.1 mention that when using communication facilities for information transport, should be taken into consideration be taken to make use of cryptographic techniques, for example to maintain confidentiality, protect the integrity and authenticity of information.

With regard to the state of the art with regard to cryptographic techniques, it is further from It is important that the National Cyber Security Center (hereinafter: NCSC) also points out the importance on its website

of protecting communications when sensitive information is sent over a connection.3

According to the NCSC, TLS (Transport Layer Security) is the most commonly used protocol for securing connections on the internet. Application of TLS to web traffic is done over the HTTPS protocol at the using a TLS certificate.

A TLS certificate can be obtained free of charge,4 although costs usually have to be incurred to having the certificate installed or renewed on the server by an IT professional because the validity period is expired. These are short-term actions that only involve labor costs.

2.3.2. Facts

[The person concerned] has stated that the website of the orthodontic practice went online on 4 June 2010.5 Because at the time of the AP's first request for information, a new website was already being worked on they referred to the then existing website as 'old website'.

The AP visited the website – which has since been replaced by another – on February 26, 2019.

It was found that the website, as stated, contained a form for the registration of new patients. This form contained fields for, among other things, the patient's contact details and his parents and the patient's BSN. The AP has also established that the website at the time of the visit did not use an encrypted connection at all. This is evident from the screenshots in appendix 9 of the research report, of which an excerpt is included below:

3 https://www.ncsc.nl/topics/connection security.

4 For example, with non-profit certificate authority Let's Encrypt, <https://letsencrypt.org/>. There are certificate authorities that are precious offer certificates (Extended Validation, or EV). Such certificates provide more information about the party to whom the certificate is issued provided, but do not lead to a different or better encryption of exchanged information.

5 Letter dated 19 August 2019, appendix 8 to the investigation report.



Date

Figure 1: Cut-out of the page formation of the website [url].

In the window shown, under the heading "Technical details" there is a message "Unencrypted connection" included. This notification reads: “The website [url] does not support encryption for the page you are viewing viewing. Data sent over the internet without encryption can continue in transit others are seen.”

[The person concerned] has acknowledged that the old website did not use an encrypted connection.6 The The developer of the old website never pointed this out to her. She certainly had otherwise used, according to [person concerned].

It follows from the letter from [person concerned] of 19 August 2019 that if a form was sent, the data was stored on the web server running the old website. The orthodontic practice received a notification. After logging in to the website, the stored data was viewed, taken over in the administration of the practice and finally removed from the web server. Between July 2018 and June 2019, the practice received no more than ten online registrations, according to [person concerned].

6 Opinion of 7 October 2019 on the intention to impose an administrative fine.



Date

February 4, 2021

Our reference

[confidential]

[The person concerned] had the old website taken offline on 29 May 2019.7

On July 4, 2019, the AP again visited the website of the orthodontic practice and found that the website, now renewed, did use an encrypted connection, but no longer one online registration form. Instead, a registration form is now offered in the form

of a PDF file, which can be downloaded, printed, completed and delivered to the practice.

2.3.3. Judgement

The question whether [data subject] has the appropriate technical and
has taken organizational measures – as stated under 2.3.1 – must be complied with
based on NEN 7510. This NEN standard has been made mandatory for the use of the BSN and for healthcare
applies that this standard also contains the accepted security standards.
The AP notes that the old website of the orthodontic practice did not have a TLS certificate and
therefore did not use the HTTPS protocol. The communication with the website, including the
sending a completed registration form, therefore proceeded over an unencrypted and therefore
unsecured connection. This created the mere availability of the registration form
an increased risk of a “man-in-the-middle attack”, where transmitted information is compromised
intercepted and read and/or modified, without the knowledge of the sending and receiving parties
of having. It has thus been established that [the person concerned] has not taken any control measures with regard to
communication security. This is not in accordance with the provisions of NEN 7510 (including de
sections 10.1 and 13.2).
It should be borne in mind that the patients of an orthodontic practice are usually minor children.
This follows from the nature of the treatment, the fields of the registration form (which asks for
the details of the parents) and the visual material on the website of the orthodontics practice. So they are
the data of these minor children that is over the unencrypted, unsecured connection
sent. In addition, it not only concerns the BSN, but also information that is closely related
to the health of the patient concerned.
Given, on the one hand, the sensitive nature of the data that could be collected via the registration form
sent, and on the other hand the state of the art and the associated very low
implementation costs of an encrypted connection, the conclusion is that [data subject] is not a suitable one
has taken technical and organizational measures to control the processing of personal data
secure against loss or unlawful processing. This means that it has Article 32, first paragraph, of the GDPR

violate.

7 Letter dated 19 August 2019, appendix 8 to the investigation report.



Date

February 4, 2021

2.3.4. View and response AP

Our reference

[confidential]

In her view of the intention to impose an administrative fine, [the person concerned] has the

presented next.

The developer of the old website never pointed out the possibility of a

encrypted connection. If she knew about it, she would certainly have used it. She is also active

tried to comply with the GDPR, by having an audit carried out every two years by a

Dutch Association of Orthodontists designated certification agency. Privacy is part of it

the audit. The latest report, dated June 2017, shows that the website has been viewed and no

comments have been made. The same certification agency provided a step-by-step plan in March 2018

to comply with the GDPR. [Involved person] has completed this plan point by point, and although attention is

devoted to privacy and information security, it is not stated that the website must use a

encrypted connection. Furthermore, [person concerned] is inspected every five years by fellow

orthodontists. Also in the last visitation report no reference was made to the lack of an encrypted

connection of the website. No one has complained to [person concerned] about security and there is support

to the best of its knowledge, suffered no damage. Finally, [person concerned] immediately took the old website offline

and commissioned to make the new website more secure.

The opinion does not lead the AP to change its position on the established violation. An audit

by a certification agency, a step-by-step plan in preparation for the application of the

GDPR and a peer review do not release [data subject], as controller, from the in

obligation laid down in Article 32, first paragraph, of the GDPR to provide the technical and

take organizational measures. That others did not point this out to her, while she did

assumed that this would happen where necessary, does not absolve it of its own responsibility to actively

to ensure the technically secure processing of personal data. An organization through

The internet processes personal data of a sensitive nature and often of children, has a large

responsibility to ensure that such personal data is also secure on it

be sent online. Incidentally, the content of the audit report and the report of the

collegial visit does not indicate that attention has been paid to protection in the context of the audit and visitation

of personal data. That no one has complained to [person concerned] and that she is not aware of any damage,

does not alter the fact that they have insufficient technical and organizational security measures

has hit.

2.3.5. Conclusion

In view of the foregoing, the AP is of the opinion that [data subject] Article 32, first paragraph, of the GDPR of

May 25, 2018 (the moment the GDPR became applicable) to May 29, 2019, because they

the website of the orthodontics practice offered a registration form that did not use a

encrypted connection while that form was intended to exchange sensitive personal data.



Date

February 4, 2021

Our reference

[confidential]

3.

3.1.

3.2.

Administrative fine

Authority of the AP to impose an administrative fine

Pursuant to Article 58, paragraph 2, preamble and under i, the AP has been read in conjunction with Article 83 of the AVG, authorized to impose an administrative fine. According to Article 83, first paragraph, an imposed fine to be effective, proportionate and dissuasive. This follows from the fourth paragraph of that provision breaches of the obligations of the controller (including those mentioned in Article 32 of the GDPR) are subject to fines of up to €10,000,000.00 or, for a company, up to 2% of the total worldwide annual turnover in the previous financial year, if this figure is higher.

Pursuant to Article 14, paragraph 3, of the General Data Protection Regulation Implementation Act (hereinafter: UAVG), in the event of a violation of the provisions of Article 83, fourth, fifth or sixth paragraph, of the GDPR, impose an administrative fine not exceeding the amount referred to in these paragraphs amounts.

When exercising the power to impose an administrative fine, the AP applies the Fining Policy Rules of the Dutch Data Protection Authority 2019 (hereinafter: Fining Policy Rules 2019).8

Penalty Policy Rules of the Dutch Data Protection Authority 2019

The relevant provisions of the Fining Policy Rules 2019 are set out in the appendix to this decision. The The system of the Fining Policy Rules 2019 is as follows.

The violations for which the AP can impose a fine up to the amount stated above are in the Fining Policy Rules 2019 divided into three fine categories. These categories are sorted by seriousness of the violation of the aforementioned articles, with category I being the least serious violations category III contains the most serious offences. The categories are subject to increasing fines connected. This follows from Article 2, under 2.1 and 2.3 of the Fining Policy Rules 2019.

Category I

Category II

Category III

Fine bandwidth between € 0 and € 200,000

Fine bandwidth between € 120,000 and € 500,000

Fine bandwidth between € 300,000 and € 750,000

Basic fine: €100,000

Basic fine: €310,000

Basic fine: €525,000

According to article 6 of the Fining Policy Rules 2019, the DPA determines the amount of the fine based on the basic fine to be adjusted upwards or downwards, depending on the extent to which the factors referred to in Article 7 give rise to this. Pursuant to Article 8, it is possible to add the next higher or lower category if the fine category determined for the violation is not appropriate in the concrete case allow punishment.

8 Published in Stcrt. 2019, 14586, March 14, 2019.



Date

February 4, 2021

Our reference

[confidential]

3.3.

Fine amount

The AP considers a fine of € 12,000.00 appropriate and necessary for the violation established above. In this is substantiated as follows in the following paragraphs. First of all, the AP sees reason for the lower penalty category I to apply. There are no fine-reducing or increasing factors that apply necessitate an adjustment of the basic fine of € 100,000.00 applicable to that fine category. Also the culpability of the conduct does not give rise to this. The AP sees reason to do so on the basis of the principle of proportionality, to moderate the fine to the aforementioned amount.

3.3.1. Fine category and basic fine

The violation of Article 32 of the GDPR (security of processing) is, according to Annex I to the Fining Policy Rules 2019, classified in category II. As follows from the table above, applies to this one category a fine range of € 120,000.00 and € 500,000.00 and a basic fine of € 310,000.00.

In this case, this fine bandwidth and basic fine cannot lead to an appropriate punishment of the detected violation. In doing so, the AP takes into account that the investigation and the violation are visible on the registration form on the website of the practice, and not on the patient administration as such. From a technical point of view, the registration form forms a separate system from that administration. The AP will therefore apply category I pursuant to Article 8 of the Fining Policy Rules 2019 (for which a fine bandwidth applies from €0.00 to €200,000.00 and basic fine of €100,000.00), and also within that category moderate the fine on the basis of what is in this and the following paragraphs considered.

The basic fine applies as a neutral starting point, and must be increased or decreased insofar as the factors listed in Article 7 of the Fining Policy Rules 2019. The final the amount of the fine must be proportionate and geared to the seriousness of the violation and the extent to which it is committed this can be blamed on the offender (compare articles 3:4 and 5:46 of the General Act administrative law; hereinafter: Awb). The factors mentioned in Article 7 give rise to the following points comments. The factors not discussed are not applicable in this case.

a. Nature, seriousness and duration of the breach

According to [person concerned], the website with the registration form went online on 27 October 2010 and on May 29, 2019 taken offline. Although the form was available for eight years and seven months use, the AP's research focused on the period from May 25, 2018 to May 29, 2019. aligns the AP with the date on which the GDPR became applicable. That means the violation, for insofar as this is taken into account, has lasted approximately one year.9 The AP considers it serious that the violation was structural and of a long duration, all the more so because [person concerned] also applied before it

9 Article 13 of the Personal Data Protection Act (hereinafter: Wbp) is materially comparable to Article 32, first paragraph, of the GDPR: both provisions require technical and organizational measures to be taken to ensure an appropriate to ensure a level of security. The interpretation of Article 13 of the Wbp is no different from that of Article 32 of the AVG in sections 2.3.2 and 2.3.3. [Person concerned] was therefore also in violation during the period that the Wbp was in force.

Date

February 4, 2021

Our reference

[confidential]

of the AVG, under the Personal Data Protection Act, was obliged to provide an appropriate
to ensure a level of security. That obligation therefore did not first arise at the time of application
become of the GDPR.

The AP charges the [person concerned] for being a professional healthcare provider in and in the run-up to the
period under investigation has not taken care of the provisions referred to in Article 32(1) of the GDPR
appropriate technical and organizational measures, through correct implementation of
NEN 7510. The BSN is obliged to do so on the basis of the Use Regulations
citizen service number in healthcare. The following applies to the other data sent via the form
that NEN 7510 contains the generally accepted security standards in healthcare. [Involved person] had here
should be aware of by virtue of its capacity as a healthcare provider.

Furthermore, [The person concerned] has not only created the theoretical possibility that the form would
are used to send sensitive data over an unsecured connection. Turned out
after all, that the form has actually been used. This applies to every entry
that the violated standard is intended to protect has come into question. Although the exact number
submissions of the form can no longer be determined, the AP considers it not unlikely that the
form was also used when the Wbp was applicable, including an appropriate one
security level was required.

The AP charges the [person concerned] with the fact that the violation took a long time and was contrary to the standards
that apply specifically to its professional group (healthcare). That the violation actually resulted
to repeatedly send sensitive data over an unsecured connection, the AP considers extra
sorry.

g. The categories of personal data affected by the breach

The registration form first asked for the citizen service number. That in itself is a sensitive issue,
but this is all the more true if the information is viewed in conjunction with the other requested information. The
sensitivity is also apparent from the legal obligation to comply with when processing the BSN
NEN 7510. Viewed in conjunction, the data provide so much information about the patient to be registered that
there is a risk of identity fraud if the data were to be intercepted. The AP takes care of that
It should also be borne in mind that this mostly concerned the data of minors, as stated in section 2.3.3.
Furthermore, the other data requested are equally sensitive because they are closely related
with the health of the patient to be registered. This also applies to registration with a
orthodontist as such. Partly because the processing no longer takes place, the AP has not investigated
whether this qualifies as special personal data as referred to in Article 9 of the GDPR, but it suffices
the finding that the form has been used to transmit sensitive personal data.
The AP charges the [data subject] that the violation relates to sensitive data
minors.



Date

February 4, 2021

Our reference

[confidential]

Increase or decrease basic fine

In view of the foregoing, the AP sees in the factors stated in the Fining Policy Rules 2019, insofar as applicable
application in the present case, no reason to reduce the basic fine. Reason for it
there is no question of increasing the fine amount either.

3.3.2. Blameability of the conduct

Pursuant to Section 5:46(2) of the Awb, when imposing an administrative fine, the AP
take into account the extent to which this can be attributed to the offender. Because in this case it's about

a violation, this is not required for the imposition of an administrative fine in accordance with established case law it is demonstrated that there is intent and the AP may assume culpability if the perpetrator is established.10

[The person concerned], as stated in paragraph 2.3.4, has referred in her opinion to an audit report, step-by-step plan to prepare for the GDPR and a report of a peer review. According to [person concerned] has it not been pointed out in any of these documents to the shortcoming with regard to the online registration form. Insofar as [the person concerned] means that there is reduced culpability because of this, the AP doesn't track her. As a care provider, she should have been professionally familiar with the care required for that care applicable security standards. The fact that others have not pointed out the shortcoming to her does not detract from it its own obligations as controller.

Now that [person concerned] can be fully blamed for the violation, the culpability of the violation is no reason to reduce the fine.

3.3.3. proportionality

Finally, the AP will assess on the basis of Articles 3:4 and 5:46 of the Awb (principle of proportionality) or the application of its policy for determining the amount of the fine given the circumstances of the specific case, does not lead to a disproportionate outcome.

In view of the proportionality of the fine to be imposed, the AP considers it important that the violation, as stated in paragraph 3.3.1, refers to the non-secure use of a registration form on the website of the practice, and not on the entire patient administration. The AP has about the use of the unsecured connection received one complaint. The AP has no information about the patient administration itself received signals and has therefore not investigated this. Furthermore, using it registration form in the period considered.

10 Compare the rulings of the CBb of 29 October 2014 (ECLI:NL:CBB:2014:395, ow. 3.5.4), 2 September 2015 (ECLI:NL:CBB:2015:312, oh. 3.7) and 7 March 2016 (ECLI:NL:CBB:2016:54, issue 8.3). Also compare the judgments of the Administrative Jurisdiction Division of

29 August 2018 (ECLI:NL:RVS:2018:2879, issue 3.2) and 5 December 2018 (ECLI:NL:RVS:2018:3969, issue 5.1). Finally, see

Parliamentary Papers II

2003/04, 29 702, no. 3, p. 134.



Date

February 4, 2021

Our reference

[confidential]

In addition, it is important that the company of [person concerned] must be classified as a medium and large company

small business (SME). It is also, given the low costs associated with secure shipping

of a form (compare section 2.3.1), not likely to be financial as a result of the violation

profits have been made or losses avoided.

In all of the circumstances stated, the AP sees reason to set the basic amount of € 100,000.

to moderate. Partly in view of the seriousness of the violation, the AP considers the substantial capacity of the

company and the target group whose personal data are processed, a fine of € 12,000.00

appropriate and required.

Finally, the AP must consider whether what [the person concerned] has put forward in its opinion op

the intention to take enforcement action, there is reason to assume that this fine will lead to a

disproportionate outcome.

[Involved person] has stated in her opinion that she will be fined the basic amount of

fine category II (€ 310,000.00) would never be able to pay. In support of that statement, she has a

provisional income tax assessment for 2018 submitted. However, it has been explained in section 3.3.1 that

not fine category II is applied, but fine category I. The associated basic amount is

in addition, this is moderated to € 12,000.00. It does not follow from the documents submitted by [involved person].

this fine would have disproportionate consequences, for example because the orthodontic practice in the

survival would be threatened. The AP therefore sees no reason in the capacity of [person concerned].

to further reduce the fine.

3.4. Conclusion

The AP sets the fine amount for the violation of Article 32, first paragraph, of the GDPR, in view of the previous fixed at € 12,000.00.



4.

Date

February 4, 2021

Our reference

[confidential]

Operative part

fine

The AP will inform [person concerned], trading under the name of [company], for violation of Article 32, first paragraph, of the AVG, an administrative fine in the amount of € 12,000.00 (in words: twelve thousand euros).11

Yours faithfully,

Authority for Personal Data,

drs. C.E. Mur

Board member

Remedies Clause

If you do not agree with this decision, you can within six weeks of the date of dispatch of the decides to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority. In accordance Article 38 of the GDPR Implementation Act suspends the operation of the GDPR by submitting a notice of objection decision to impose the administrative fine. State in your notice of objection at least:

- your name and address;
- the date of your objection;
- the reference mentioned in this letter (case number), or enclose a copy of this decision;

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

 your signature.

You can submit the notice of objection digitally via the website. Go to www.autoreitpersonal data.nl, and

click on the link at the bottom of the page, under the heading "Contact with the Dutch Data Protection Authority".

“Appeal against a decision”. From there you use the “Appeal form”.

Do you prefer to send the notice of objection by post? Then it can be sent to the following address:

Authority for Personal Data

Directorate of Legal Affairs & Legislative Advice, Objection Department

PO Box 93374

2509 AJ THE HAGUE

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



Date

February 4, 2021

Our reference

[confidential]

APPENDIX – Legal framework

General Data Protection Regulation (GDPR)

Article 2 (Material scope

1. This Regulation applies to wholly or partially automated processing,

as well as to the processing of personal data that are included in a file or that are intended

to be included in it.

[…]

Article 3 (Territorial scope

1. This Regulation applies to the processing of personal data in the context of the

activities of an establishment of a controller or processor in the Union,

whether or not the processing takes place in the Union.

[…]

Article 4 (Definitions)

For the purposes of this Regulation:

1)

"personal data" means any information relating to an identified or identifiable natural person

("the data subject"); an identifiable natural person is considered to be directly or indirectly

can be identified, in particular by an identifier such as a name, a

identification number, location data, an online identifier or one or more elements that

be characteristic of the physical, physiological, genetic, psychological, economic, cultural or

social identity of that natural person;

"processing" means any operation or set of operations relating to personal data or

a set of personal data, whether or not carried out by automated processes, such as the

collecting, recording, organizing, structuring, storing, updating or changing, retrieving, consulting,

use, provide by transmission, distribution or otherwise available

compile, align or combine, block, erase or destroy data;

2)

[…]

7)

"controller" means a natural or legal person, a public authority,

a service or other body that, alone or jointly with others, achieves the ends and means

for the processing of personal data; when the objectives of and the means

can be laid down in Union law or Member State law for this processing

determine who the controller is or according to which criteria it will be

designated;

[…]

Article 32 (Processing security)

1. Taking into account the state of the art, the implementation costs, as well as the nature, the

scope, context and processing purposes and the likelihood and severity

various risks to the rights and freedoms of individuals affect the



Date

February 4, 2021

Our reference

[confidential]

controller and the processor appropriate technical and organizational

measures to ensure a level of security appropriate to the risk, which, where appropriate,

include, among others:

a) the pseudonymization and encryption of personal data;

b) the ability to maintain on an ongoing basis the confidentiality, integrity, availability and

ensure resilience of processing systems and services;

c) the ability to ensure the availability of and access to in the event of a physical or technical incident

to restore the personal data in a timely manner;

d) a procedure for testing, assessing and evaluating the

effectiveness 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 deletion

unauthorized disclosure of or unauthorized access to transmitted, stored or

otherwise processed data, whether accidentally or unlawfully.

[…]

Article 58 (Powers)

[…]

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

measures:

[…]

i) according to the circumstances of each case, in addition to or instead of those referred to in this paragraph

measures, impose an administrative fine under Article 83; and

[…]

[…]

Article 83 (General conditions for imposing administrative fines)

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

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

be effective, proportionate and dissuasive in each case.

2. Administrative fines shall, depending on the circumstances of the case, be

imposed in addition to or instead of those referred to in points (a) to (h) and (j) of Article 58(2).

measures. When deciding whether to impose an administrative fine and on the

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

a) the nature, gravity and duration of the breach, taking into account the nature, scale or

purpose of the processing in question as well as the number of data subjects affected and the extent of

the damage suffered by them;

b) the intentional or negligent nature of the breach;



Date

February 4, 2021

Our reference

[confidential]

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 that he has implemented in accordance with the

articles 25 and 32;

e) previous relevant breaches by the controller or processor;

f)

the degree of cooperation with the supervisory authority to prevent the breach

rectify and limit the possible negative consequences thereof;

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

h) the manner in which the supervisory authority became aware of the breach, in particular

whether, and if so to what extent, the controller or processor has the breach

reported;

compliance with the measures referred to in Article 58(2), insofar as those earlier concerned

of the controller or processor in question with regard to the same

matter have been taken;

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

certification mechanisms in accordance with Article 42; and

i)

j)

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

factor, such as financial gains made, or losses avoided, which may or may not result directly

result from the infringement.

Violations 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 the total worldwide

annual turnover in the previous financial year, if this figure is higher:

a) the obligations of the controller and the processor in accordance with the

Articles 8, 11, 25 to 39, and 42 and 43;

[…]

[…]

4.

[…]

Implementation Act General Data Protection Regulation

Article 14 (Tasks and powers)

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

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

[…]

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 specified in this

amounts mentioned by members.

[…]



Date

February 4, 2021

Our reference

[confidential]

Supplementary provisions on the processing of personal data in healthcare12

Article 8

1. The healthcare provider will include the client's citizen service number in its administration with the

recording personal data with regard to the provision of care.

decree: Decree on the use of citizen service numbers in healthcare;

[…]

Article 10

The security requirements for data processing can be determined by ministerial regulation

in Articles 8 and 9.

Scheme for using citizen service number

Article 1

In this regulation the following definitions apply:

a. Minister: Minister of Health, Welfare and Sport;

b. Act: Use of Citizen Service Number in Healthcare Act;13

c.

d. NEN: standard issued by the Netherlands Standardization Institute;

e. NEN 7510: NEN 7510 and its elaborations in NEN 7511 and NEN 7512;

[…]

Article 2

The data processing referred to in Articles 8 and 9 of the Act [...] complies with NEN 7510.

NEN 7510-2: Medical informatics - Information security in healthcare -

Part 2: Control measures

10.1.1 Policy on Use of Cryptographic Controls

Control measure

Information protection includes a cryptographic use policy

control measures to be developed and implemented.

[…]

When implementing the cryptography policy, the

regulations and national restrictions that may apply to the use of cryptographic

techniques in different parts of the world and with cross-border issues

12 Until 1 July 2017, this law was called the Use of Citizen Service Number in Healthcare Act.

13 As stated in the footnote above, this Act is now known as the Additional Provisions for the Processing of Personal Data Act

the care.

Date

February 4, 2021

Our reference

[confidential]

streams of encrypted information (see 18.1.5).

Cryptographic controls can be used for a variety of purposes

information security objectives, e.g.:

a) confidentiality: using encryption of information to protect sensitive or essential information,

during storage or shipping;

[…]

Other information

Decision making about whether a cryptographic solution is appropriate should be made

considered part of the overall process of risk assessment and control selection.

[…]

For choosing the right cryptographic control measures that meet the objectives

of the information security policy, expert advice should be sought.

13.2.1 Information Transport Policies and Procedures

Control measure

In order to protect the information transport, which goes through all types of communication facilities,

formal transportation policies, procedures, and controls should be in place.

Implementation guideline

In procedures to be followed and control measures to be carried out at

the use of communication facilities for information transport includes the following points

to be taken into consideration:

a) procedures designed to secure transferred information against interception,

copying, alteration, misrouting and destruction;

[…]

f) use of cryptographic techniques, e.g. to ensure confidentiality, integrity and authenticity

of information (see Chapter 10);

[…]

CARE SPECIFIC IMPLEMENTATION GUIDELINE

Organizations should ensure the security of such information exchange

is the subject of policy development and compliance audits (see Chapter 18).

[…]

18/20

Date

February 4, 2021

Our reference

[confidential]

Penalty Policy Rules of the Dutch Data Protection Authority 2019

Article 2. Category classification and penalty ranges

2.1 The provisions with regard to violations of which the Dutch Data Protection Authority has issued an administrative order

can impose a fine of up to € 10,000,000 or, for a company, up to 2%

of the total worldwide annual turnover in the previous financial year, whichever is higher, are in

annex 1 classified in category I, category II or category III.

[…]

2.3 The Dutch Data Protection Authority sets the basic fine for violations for which a statutory

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

annual turnover in the previous financial year, if this figure is higher, or € 20,000,000 or, for a

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

figure is higher, fixed within the following fine ranges:

Fine bandwidth between € 0 and € 200,000

Fine bandwidth between € 120,000 and € 500,000

Fine bandwidth between € 300,000 and € 750,000

Basic fine: €100,000

Basic fine: €310,000

Basic fine: €525,000

Category I

Category II

Category III

[…]

2.4 The amount of the basic fine is set at the minimum of the bandwidth increased

with half the bandwidth of the penalty category linked to a violation.

Article 6. The basic fine and possible increase or reduction

The Dutch Data Protection Authority determines the amount of the fine by the amount of the basic fine

above (up to the maximum of the bandwidth of the violation linked

penalty category) or downwards (to at least the minimum of that bandwidth). The

base fine is increased or decreased depending on the extent to which the factors mentioned in

Article 7 give rise to this.

Article 7. Relevant Factors

Without prejudice to Sections 3:4 and 5:46 of the General Administrative Law Act, the Authority

Personal data take into account the factors referred to under a to k, insofar as they are concrete

case of application:

a) the nature, gravity and duration of the breach, 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 processing by them

damages suffered;

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 of the General Data Protection Regulation;

previous relevant breaches by the controller or processor;

e)



Date

February 4, 2021

Our reference

[confidential]

f)

the degree of cooperation with the supervisory authority to remedy the breach

and limit the possible negative consequences thereof;

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

h) the manner in which the supervisory authority became aware of the breach, in particular whether,

i)

j)

and if so, to what extent, the controller or processor has notified the breach;

compliance with the provisions of Article 58, paragraph 2, of the General Data Protection Regulation

the aforementioned measures, insofar as they have previously been applied to the controller or the

processor in question in respect of the same matter;

adherence to approved codes of conduct in accordance with article 40 of the General

data protection regulation or approved certification mechanisms accordingly

Article 42 of the General Data Protection Regulation; 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.

Article 8. Going outside the bandwidth and increased maximum fines for a company

8.1 If the fine category determined for the violation is not appropriate in the concrete case

permits punishment, the Dutch Data Protection Authority can determine the amount of the fine

penalty bandwidth of the next higher category, respectively, the penalty bandwidth of the next

apply lower category

Annex 1, belonging to Article 2

Violations with a legal maximum fine of €10,000,000 or, for a company, up to 2% of

the total worldwide annual turnover in the previous financial year, if this figure is higher:

Description

Article of law

General Data Protection Regulation

[…]

article 32

[…]

[…]

security of processing

[…]

Category

[…]

II

[…]