Confidential/Registered

[CONFIDENTIAL]

Date

February 4, 2021

Our reference

[confidential]

Contact

[confidential]

Topic

Decision to impose an administrative fine

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authority data.nl

Dear [person concerned],

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 has not complied with your obligation to provide appropriate technical information when processing personal data and organizational measures (Article 32, first paragraph, 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 violation detected. In section 3, discussed the authority of the AP to impose a fine, and the amount of the fine. Paragraph 4 finally contains the decision (the operative part) and the remedies clause.

Introduction

1.

1.1. About the offender

The company “[company]” is run by [person concerned]. On the website of the orthodontic practice it is stated that, in addition to [the person concerned] as an orthodontist, the practice has eleven employees.

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].

Date

February 4, 2021

Our reference

[confidential]

1.2.

2.

2.1.

Reason for the investigation and the course of the proceedings

On November 27, 2018, the AP received a complaint as referred to in Article 77 of the GDPR. According to the complaint will be sensitive data via the registration form on the website of the orthodontic practice requested, such as the citizen service number (hereinafter: BSN), but the data is subsequently sent unencrypted.

The AP visited the website of the orthodontics practice on February 26, 2019 and screenshots of it created.

In a letter dated 29 May 2019, the AP requested [the person concerned] for information. [Involved person] has letter of June 4, 2019.

The AP visited the website of the orthodontics practice again on July 4, 2019 and screenshots of it created.

In a letter dated 12 August 2019, the AP requested [the person concerned] for further information. [Data Subject] responded to this in a letter dated 19 August 2019.

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

In a letter dated 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 [the person concerned] in the given the opportunity to comment on it.

By letter dated 7 October 2019, supplemented by those dated 9 and 12 December 2019, [the person concerned] submitted a opinion submitted.

Facts and Review

The relevant legislation and regulations are listed in the appendix to this Decree.

Processing of personal data

At the time of the complaint, the orthodontic practice's website contained a registration form 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 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 thus personal data as referred to in Article 4, preamble and under 1 of the GDPR.

It follows from [the person concerned]'s letter of 19 August 2019 that after sending the form, the completed data was 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. Subsequently,

the data stored online has been removed, according to [the 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, opening words 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 the orthodontic practice run as a sole proprietorship, required for the treatment and financial handling thereof. [Data subject] is thus the controller, referred to in Article 4, preamble and under 7 of the GDPR.

2.2.

2.3. Violation related to the security of the processing

2.3.1. Introduction

The controller is obliged, pursuant to Article 32(1) of the GDPR, to:

to take appropriate technical and organizational measures to prevent the processing of personal data to protect against, among other things, loss or unlawful processing of the data. These measures must ensure 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 of whether the controller has the referred to in Article 32(1) of the GDPR has taken measures, will be assessed as follows in cases such as the present one. The processing of the BSN of a patient by a healthcare provider must comply with NEN 7510. That is a information security standard for healthcare. 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 of this statutory obligation with regard to the citizen service number, for healthcare, NEN 7510 applies the general 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, first paragraph, 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 submission of the required

data, such as the citizen service number (BSN). Compare the drafting history of this provision (Parliamentary Papers II 2005/06, 30 380, no. 3, p. 20).

2 Compare the Dutch DPA Guidelines for the Security of Personal Data (Government Gazette 2013 no. 5174, p. 11).

Date

February 4, 2021

Our reference

[confidential]

protect the confidentiality, authenticity and/or integrity of information. In section 10.1.1,

state that to protect information, a policy on the use of cryptographic

control measures should be developed and implemented. These can include

be used for the purpose of maintaining confidentiality by preventing the encryption of information

to protect sensitive or critical information, whether in storage or transmission.

Chapter 13 of NEN 7510-2 discusses control measures with regard to

communication security. Section 13.2 contains control measures with regard to

information transport. The purpose of these controls is to maintain the security of

information exchanged within an organization and with an external entity. In section 13.2.1

states that when using communication facilities for information transport, consideration should be given to

be taken to make use of cryptographic techniques, for example to ensure confidentiality,

protect the integrity and authenticity of information.

With regard to the state of the art with regard to cryptographic techniques, it is further

importance 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 widely used protocol for securing connections on the Internet. Application of TLS to web traffic is done via the HTTPS protocol at the using a TLS certificate.

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

2.3.2. Facts

[The person concerned] stated that the website of the orthodontic practice went online on 4 June 2010.5

Because a new website was already being worked on at the time of the AP's first information request, they referred to the then existing website as the 'old website'.

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

It was noted that, as stated, the website contained a form for the registration of new patients. This form contained fields for, among other things, the patient's contact details and the patient's parents and 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/onderwerpen/binding security.

4 For example with non-profit certificate authority Let's Encrypt, < https://letsencrypt.org/>. There are certificate authorities that provide precious offer certificates (Extended Validation, or EV). Such certificates provide more information about the party to whom the certificate is 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.

Figure 1: Excerpt of the page formation of the website [url].

In the window shown under the heading “Technical details” there is a message “Unencrypted connection”

Hospitalized. This message reads: “The website [url] does not support encryption for the page you

viewing. Data sent over the internet without encryption can pass through in transit

others are seen.”

[The person concerned] acknowledged that the old website did not use an encrypted connection.6 The

developer of the old website never pointed out that possibility to her. Otherwise she certainly would have

made use of, according to [the person concerned].

It follows from [the person concerned]'s letter 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 [the person concerned].

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

Date

February 4, 2021

Our reference

[confidential]

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

The AP visited the website of the orthodontic practice again on July 4, 2019 and found that the

website, now renewed, did use an encrypted connection, but no longer a

includes online registration form. Instead, a registration form is now offered in the form
from a PDF file, which can be downloaded, printed, completed, and delivered to the practice.

2.3.3. Rating

The question whether [the person concerned] has the appropriate technical and
has taken organizational measures must – as stated under 2.3.1 – comply with
based on NEN 7510. This NEN standard has been made mandatory for the use of the BSN and for the care
applies that this standard also contains the accepted security standards.

The AP establishes that the old website of the orthodontic practice did not have a TLS certificate and
therefore did not use the HTTPS protocol. Communication with the website, including the
sending a completed registration form, therefore took place over an unencrypted and therefore
unsecured connection. Because of this, the mere having the registration form available
an increased risk of a “man-in-the-middle attack”, where information is sent
intercepted and read and/or changed, without the sending and receiving party knowing
of having. It is thus 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 the
paragraphs 10.1 and 13.2).

It should be borne in mind that the patients of an orthodontic practice are generally 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 images on the website of the orthodontic practice. So they are
the data of these minor children over the unencrypted, unsecured connection
sent. In addition, this does not only concern the citizen service number (BSN), but also data that are 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 minor
implementation costs of an encrypted connection, the conclusion is that [data subject] does not have an appropriate
has taken technical and organizational measures to prevent the processing of personal data

protect it against loss or unauthorized processing. It thus has Article 32, first paragraph, of the GDPR violate.

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

2.3.4. View and response AP

In its view of the intention to impose an administrative fine, [the person concerned] has brought forward next.

The developer of the old website never pointed out to [the person concerned] the possibility of a encrypted connection. If she knew about it, she would certainly have used it. Furthermore, she has actively tried to comply with the GDPR by having an audit performed every two years by a Dutch Association of Orthodontists designated certification agency. Privacy is part of the audit. The latest report, dated June 2017, shows that the website has been viewed and that 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 visited 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 has been to the best of its knowledge suffered no damage. Finally, [person involved] immediately took the old website offline and commissioned the new website to be more secure.

The opinion does not lead the AP to a different position on the violation that has been established. 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 discharge [data subject], as controller, from the in

obligation laid down in Article 32(1) of the GDPR to carry out the technical and

organizational measures. That others have not pointed this out to her, while she

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

to ensure a technically secure processing of personal data. An organization that

processing personal data of a sensitive nature and often of children on the internet has a significant

responsibility to ensure that such personal data is also

be sent over the internet. Incidentally, it appears from the content of the audit report and the report of the

peer review not that attention has been paid to protection in the context of the audit and review

of personal data. That no one has complained to [the person concerned] and that no damage is known to her,

also does not alter the fact that they do not have sufficient technical and organizational security measures

has hit.

2.3.5. Conclusion

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

May 25, 2018 (when the GDPR came into effect) until May 29, 2019, because they acted on

the website of the orthodontic 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

Power of the AP to impose an administrative fine

Pursuant to Article 58, second paragraph, 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. It follows from the fourth paragraph of that provision that breaches of the controller's obligations (including those referred to in Article 32 of the GDPR) are subject to fines up to € 10,000,000.00 or, for a company, up to 2% of the total worldwide annual turnover in the previous financial year, whichever is higher.

Pursuant to Article 14, paragraph 3, of the General Data Protection Regulation Implementing Act (hereinafter: UAVG) in the event of violation of the provisions of Article 83, fourth, fifth or impose an administrative fine of a maximum of the referred to in these paragraphs, paragraph 6 of the GDPR amounts.

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

Fine policy rules of the Dutch Data Protection Authority 2019

The relevant provisions of the 2019 Fine Policy Rules are listed in the appendix to this Decree. The The system of the 2019 Fine Policy Rules is as follows.

The violations for which the AP can impose a fine up to the amount stated above are in the Fines policy rules 2019 divided into three fine categories. These categories are arranged according to gravity of the violation of the aforementioned articles, with category I the least serious violations contains and category III 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 Fine 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 Fine Policy Rules 2019, the AP determines the amount of the fine by means of the basic fine 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 assign the next higher or lower category to be applied if the fine category determined for the violation is not appropriate in the specific case permitting 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 appropriate for the violation noted above. In In the following paragraphs, this is substantiated as follows. First of all, the AP sees reason to lower the fine category I. There are no fine reducing or increasing factors applicable that necessitate an adjustment of the basic fine of € 100,000 that applies to that fine category. Also the culpability of the conduct does not give rise to this. The AP does see reason to of the principle of proportionality to reduce 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 Fines Policy Rules 2019, classified in category II. As follows from the table above, for this

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. The AP takes into account that the investigation and the violation
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 on the basis of Article 8 of the Fine Policy Rules 2019 (for which a
fine range applies from €0.00 to €200,000.00 and basic fine of €100,000.00), and also within that
category moderate the amount of the fine on the basis of what is stated 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 in
Article 7 of the Fines Policy Rules 2019 give rise to this. The final
the amount of the fine must be proportionate and geared to the seriousness of the violation and the extent to which
this can be blamed on the offender (compare Articles 3:4 and 5:46 of the General Law
administrative law; hereinafter: Awb). The factors listed in Article 7 give rise to
comments. The factors not discussed do not apply in this case.

a. Nature, seriousness and duration of the infringement

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

9 Article 13 of the Personal Data Protection Act (hereinafter: Wbp) is materially comparable to Article 32(1) of
the GDPR: both provisions oblige 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 GDPR,
described

in paragraphs 2.3.2 and 2.3.3. The [person concerned] was therefore also in violation during the period that the Wbp applied.

Date

February 4, 2021

Our reference

[confidential]

under the GDPR, on the basis of the Personal Data Protection Act, was obliged to provide an appropriate
to ensure a level of security. That obligation therefore did not arise when the
become of the GDPR.

The AP charges the [person concerned] that she acts as a professional care provider in and in the run-up to the
investigated period has not taken care of the provisions referred to in Article 32(1) of the GDPR
appropriate technical and organizational measures, through proper implementation of
NEN 7510. The BSN is obliged to do so on the basis of the Regulation on use
citizen service number in healthcare. For the other data sent via the form, the following applies:
that NEN 7510 contains generally accepted security standards in healthcare. [Involved person] had here
by virtue of her capacity as a healthcare provider.

[The person concerned] has furthermore not only created the theoretical possibility that the form would
are used to send sensitive data over an unsecured connection. It has been found
after all, that the form has actually been used. For each submission, the importance of
that the breached standard seeks to protect has been compromised. Although the exact number
submissions of the form can no longer be determined, the AP does not consider it unlikely that it
form was also used when the Wbp was applicable, including an appropriate
security level was required.

The AP charges the [person concerned] that the violation lasted a long time and was contrary to the standards
that apply specifically to her professional group (care). That the violation actually led
to repeatedly sending sensitive data over an unsecured connection, the AP deems extra

sorry.

g. The categories of personal data to which the breach relates

First, you were asked for your citizen service number (BSN) via the registration form. That in itself is a sensitive matter.
but this applies all the more if the data is viewed in conjunction with the other requested data. The
sensitivity is also apparent from the legal obligation to comply with the BSN when processing the citizen service number
NEN 7510. Viewed together, the data provide so much information about the patient to be registered that
there is a risk of identity fraud if the data were intercepted. The AP takes
also take into account that this mostly concerned the data of minors, as stated in section 2.3.3.
Furthermore, the other data requested are also of a sensitive nature, as they are closely related
with the health of the patient to be enrolled. This also applies to registration with a
orthodontist as such. The AP has not investigated, partly because the processing no longer takes place
whether this qualifies as special personal data as referred to in Article 9 of the GDPR, but is sufficient with
the finding that the form has been used to send sensitive personal data.
The AP charges the [person concerned] that the violation relates to sensitive data of
minors.

Date

February 4, 2021

Our reference

[confidential]

Increase or decrease basic fine

In view of the foregoing, the AP considers the factors stated in the 2019 Fine Policy Rules, to the extent of
applicable in the present case, there is no reason to reduce the basic fine. Due to the
there is also no question of increasing the amount of the fine.

3.3.2. culpability of the conduct

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

into account the extent to which this can be blamed on the offender. Because in this case it's about
a violation, for the imposition of an administrative fine, in accordance with established case law, it is not required that
it is demonstrated that there is intent and the AP may presume culpability if it
offense is established.10
As stated in paragraph 2.3.4, [Involved person] has referred to an audit report in her opinion,
step-by-step plan for preparing for the GDPR and a report of a peer visitation. According to [person involved]
has it not been pointed out in any of these documents of the shortcoming with regard to the online
registration form. Insofar as [the person concerned] means that this means that there is reduced culpability,
the AP does not follow her. As a care provider, she should have been professionally familiar with the care required for that care
applicable security standards. It doesn't change the fact that others have not pointed out the shortcoming to her
its own obligations as a data controller.
Now that [the person concerned] can be fully blamed for the violation, the culpability of the
violation is not a 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 the light 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 control over the patient administration itself
received signals and therefore did not investigate them. Furthermore, the use of the
registration form in the considered period remained limited.
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,
ow. 3.7) and 7 March 2016 (ECLI:NL:CBB:2016:54, ow. 8.3). Also compare the judgments of the Administrative Jurisdiction

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

Parliamentary Papers II

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

It is also important that the company of [the person concerned] must be classified as medium and

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

of a form (compare paragraph 2.3.1), not plausible that as a result of the violation financial

profits have been made or losses have been avoided.

In all of the circumstances mentioned, the AP sees reason to apply the basic amount of € 100,000

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

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

appropriate and appropriate.

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

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

would lead to a disproportionate outcome.

[The person concerned] has stated in her opinion that she has to pay a fine in the amount of the basic amount of

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

provisional income tax assessment for 2018 submitted. However, it is explained in paragraph 3.3.1 that

fine category II is not applied, but fine category I. The corresponding base amount is

moreover moderated to € 12,000.00 for this. It does not follow from the documents submitted by [the person concerned] that

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 [the person concerned]

to further mitigate the fine.

3.4. Conclusion

The AP sets the fine 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]

dictum

fine

The AP submits to [the person concerned], acting under the name of [company], for violation of Article 32,

first paragraph, of the GDPR, an administrative fine in the amount of € 12,000.00 (in words: twelve thousand euros).11

Yours faithfully,

Authority Personal Data,

drs. C.E. Mur

board member

Remedies Clause

If you do not agree with this decision, you can cancel within six weeks of the date of dispatch of the

decide to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority. In accordance with

Article 38 of the GDPR Implementation Act suspends the operation of the

decision to impose the administrative fine. In your notice of objection, state at least:

 your name and address;

 the date of your notice of objection;

 the reference (case number) mentioned in this letter, or enclose a copy of this decision;

 the reason(s) why you do not agree with this decision;

 your signature.

You can submit the notice of objection digitally via the website. Go to www.autoreitbedrijven.nl, en

Click at the bottom of the page, under the heading “Contact with the Dutch Data Protection Authority”, on the link

“Objection to a decision”. From there, use the “Objection Form”.

Would you rather send the notice of objection by post? Then you can send it to the following address:

Authority for Personal Data

Legal Affairs & Legislative Advice Department, Objections Department

PO Box 93374

2509 AJ THE HAGUE

11 The AP will hand the claim over 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 processing wholly or partly by automated means,

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

to be included therein.

[…]

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,

regardless of whether the processing takes place in the Union or not.

[…]

Article 4 (Definitions)

For the purposes of this Regulation:

1)

"personal data": any information about an identified or identifiable natural person

("the data subject"); is considered identifiable a natural person who directly or indirectly

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

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

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

social identity of that natural person;

"processing" means an operation or set of operations on personal data or

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

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

use, provide by transmission, dissemination or otherwise make available

set, align or combine, shield, erase or destroy data;

2)

[…]

7)

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

a service or other body which, alone or jointly with others, has the purpose and means of

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

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

determine who the controller is or according to what criteria it is

designated;

[…]

Article 32 (Security of processing)

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

scope, context and purposes of processing 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 the following:

a) the pseudonymisation 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, in the event of a physical or technical incident, to control the availability of and access to

to restore the personal data in a timely manner;

d) a procedure for the regular testing, assessment and evaluation of the

effectiveness of 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 disclosure of or access to any transmitted, stored or

otherwise processed data, whether accidentally or unlawfully.

[…]

Article 58 (Powers)

[…]

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

measures:

[…]

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

measures, impose an administrative fine under Article 83; and

[…]

[…]

Article 83 (General conditions for the imposition of administrative fines)

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

this Article 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, depending on the circumstances of the individual case, are

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

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

amount, due account shall be taken of the following in each specific case:

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

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

the damage suffered by them;

b) the intentional or negligent nature of the infringement;

Date

February 4, 2021

Our reference

[confidential]

c) the measures taken by the controller or processor to

limit the damage suffered by those involved;

d) the extent to which the controller or processor is responsible in view of the

technical and organizational measures that he has carried out in accordance with the

Articles 25 and 32;

e) previous relevant breaches by the controller or processor;

f)

the extent to which there has been cooperation with the supervisory authority to prevent the infringement

remedy and limit the possible negative consequences thereof;

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

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

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

reported;

compliance with the measures referred to in Article 58(2), in so far as they are earlier with regard to

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 applicable to the circumstances of the case

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

result from the infringement.

Infringements of the provisions below are subject to administrative

fines up to EUR 10 000 000 or, for a company, up to 2 % of the total worldwide

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

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

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

[…]

[…]

4.

[…]

Implementation Act General Data Protection Regulation

Article 14 (Duties and powers)

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

exercises 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(4),

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

members mentioned amounts.

[…]

Date

February 4, 2021

Our reference

[confidential]

Supplementary Provisions for the Processing of Personal Data in Healthcare12

Article 8

1. The healthcare provider records the client's citizen service number in its administration at the

recording personal data with regard to the provision of care.

decision: Decision to use citizen service number in healthcare;

[…]

Article 10

It can be determined by ministerial regulation which security requirements the data processing referred to is

in Articles 8 and 9.

Regulations for the use of citizen service number

Article 1

In this scheme, the following definitions apply:

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

b. law: Use of citizen service number in healthcare;13

c.

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

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 the use of cryptographic controls

Control measure

To protect information, a policy on the use of cryptographic

control measures to be developed and implemented.

[…]

The implementation of the cryptography policy should take into account the

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

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

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

13 As stated in the footnote above, this law is now called the Act on additional provisions for the processing of personal data in

the care.

17/20

Date

February 4, 2021

Our reference

[confidential]

streams of encrypted information (see 18.1.5).

Cryptographic controls can be used for various

information security objectives, e.g.:

a) Confidentiality: Using encryption of information to protect sensitive or essential information,

during storage or shipment;

[…]

Other information

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

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

[…]

For choosing the right cryptographic controls that meet the objectives

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

13.2.1 Information transfer policies and procedures

Control measure

To protect the information transport, which takes place through all types of communication facilities,

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

Implementation guideline

In procedures that must be followed and control measures that must be carried out at

the use of communication facilities for information transport, the following points include:

to be considered:

a) procedures designed to protect transferred information from interception,

copying, modification, 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 that the security of such exchange of information is

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

[…]

18/20

Date

February 4, 2021

Our reference

[confidential]

Fine policy rules of the Dutch Data Protection Authority 2019

Article 2. Category classification and penalty bandwidths

2.1 The provisions regarding violations of which the Dutch Data Protection Authority has an administrative

can impose a fine not exceeding the amount of € 10,000,000 or, for a company, up to 2%

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

appendix 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 total worldwide annual sales in the previous fiscal year, if

number is higher, fixed within the following penalty 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 fine 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 dividing the amount of the basic fine to

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

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

basic 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 Articles 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 in the concrete

case of application:

(a) the nature, gravity and duration of the infringement, taking into account the nature, extent 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 infringement;

c) the measures taken by the controller or processor to

limit the damage suffered by those involved;

d) the extent to which the controller or processor is responsible in view of the

technical and organizational measures that he has implemented in accordance with Articles 25

and 32 of the General Data Protection Regulation;

previous relevant breaches by the controller or processor;

e)

Date

February 4, 2021

Our reference

[confidential]

f)

the extent to which there has been cooperation with the supervisory authority to remedy the infringement

and limit the possible negative consequences thereof;

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

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

i)

j)

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

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

the aforementioned measures, insofar as they were previously addressed to the controller or the

processor in question with regard to the same matter;

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

Data Protection Regulation or of approved certification mechanisms in accordance with

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, whether directly or indirectly from the infringement

result.

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

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

punishment permits, the Dutch Data Protection Authority may, when determining the amount of the fine,

fine bandwidth of the next higher category or the fine bandwidth of the next

apply lower category

Annex 1, belonging to Article 2

Violations with 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:

Description

Article of law

General Data Protection Regulation

[…]

article 32

[…]

[…]

processing security

[…]

Category

[…]

II

[…]