Confidential/Registered

CP&A B.V.

attn. the direction

PO Box 514

5600 AM Eindhoven

Date

March 24, 2020

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Topic

Decision to impose an administrative fine

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authority data.nl

Dear management,

The Dutch Data Protection Authority (AP) has decided to inform CP&A B.V. (CP&A) an administrative fine of €15,000 to be imposed. The AP believes that CP&A will suspend the ban from March 12, 2019 to May 2, 2019. of Article 9, first paragraph, of the General Data Protection Regulation (GDPR) by processing health data of its employees. In addition, CP&A has for this processing during the same period did not take adequate security measures if referred to in Article 32(1) of the GDPR.

The decision is explained in more detail below. Chapter 1 is an introduction and chapter 2 describes it

legal framework. Chapter 3 contains the facts and in chapter 4 the DPA assesses whether there is processing of health data, the processing responsibility and the violations. In Chapter 5 sets out the (amount of the) administrative fine and Chapter 6 contains the operative part and the remedies clause.

1 Introduction

1.1 Legal entity involved and reason for investigation

CP&A is a private company with its registered office at Maas 22E, 5684 PL in Best (North Brabant). CP&A is registered in the trade register of the Chamber of Commerce under number 54592526 and, according to the extract from the trade register, employs approximately 160 people. CP&A performed according to the trade register and its website, among other things, inspection and maintenance work of public objects.

The AP received a notification on January 11, 2019 that CP&A is processing health data from its employees. The AP supervisors concluded from the report that CP&A is an online maintains absenteeism registration containing health data of sick employees. In response to this signal, the AP has launched an (official) investigation into CP&A's compliance with Articles 9 and 32 of the GDPR.

The processing of special categories of personal data is subject to Article 9, first paragraph, of prohibited by the GDPR, unless a legal exception applies. The AP tests in the following whether CP&A can successfully invoke the exception relevant to this case. In addition, the AP or CP&A for the health data in its absenteeism registration sufficiently appropriate technical and has taken organizational measures to ensure a security level appropriate to the risk

safeguards, as referred to in Article 32(1) of the GDPR.

1.2 Process

The AP contacted CP&A by telephone on 2 May 2019 to indicate that the

CP&A's absenteeism registration is accessible to unauthorized persons and it has requested CP&A to

violation as soon as possible. On 2 May 2019, following the telephone call, the AP

conversation sent a norm-transferring letter and the legal framework with regard to the reporting obligation of

explained personal data breaches to the AP. By letter dated 7 May 2019, CP&A has de

receipt of the letter and indicated that the absence registration has been deleted.

On May 7, 2019, CP&A filed a data breach notification regarding the breach related to

personal data.

In a letter dated 29 July 2019, the AP asked CP&A questions, to which it responded by letter dated 7

August 2019. On August 21, 2019, the AP requested further information from CP&A by email.

CP&A responded by email dated August 28, 2019.

In a letter dated October 30, 2019, the AP sent CP&A an intention to enforce and comply with it

sent the basis of the investigation report and gave CP&A the opportunity to submit a

expressing the point of view. On November 12, 2019, CP&A submitted a written opinion

created. Finally, on January 30, 2020, the AP added further documents to the file and CP&A de

given the opportunity to respond to these documents. CP&A has not made use of this.

2. Legal framework

2.1 Scope GDPR

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

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

included or intended to be included therein.

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

personal data in the context of the activities of an establishment of a

controller or a processor in the Union, whether or not the processing is carried out in the Union

does not take place.

Pursuant to Article 4 of the GDPR, for the purposes of this Regulation:

1. “Personal data”: any information about an identified or identifiable natural person

(“the data subject”); […].

2. “Processing”: an operation or set of operations relating to personal data or

a set of personal data, whether or not carried out by automated processes […].

7. “Controller” means a […] legal entity that, alone or jointly with others, fulfills the purpose of

and determine the means of processing personal data; […].

2.2 Prohibition of processing health data

Article 4(15) of the GDPR defines health data as personal data that

relating to the physical or mental health of a natural person, including data

on health services provided that provide information about his health status.

Pursuant to Article 9(1) of the GDPR, the processing of health data is prohibited.

Exceptions to the prohibition to process special personal data are stated in Article 9.

second paragraph of the GDPR. In so far as relevant, that provision reads:

[…]

b) the processing is necessary for the performance of obligations and the exercise of

specific rights of the controller or data subject with regard to the

labor law and social security and social protection law, to the extent permitted by

Union or Member State law or by collective agreement under Member State law which

provides appropriate safeguards for the fundamental rights and interests of the data subject;

Date

March 24, 2020

Our reference

[CONFIDENTIAL]

[…]

Pursuant to Article 30 of the Implementing Act of the General Data Protection Regulation (UAVG), the Article 9(2)(b) of the GDPR does not prohibit the processing of health data applicable if the processing is carried out by administrative bodies, pension funds, employers or institutions working on their behalf, and insofar as the processing is necessary for:

[…]

b. the reintegration or guidance of employees or beneficiaries in connection with illness or incapacity for work.

[…]

2.3 Processing security

Pursuant to Article 32(1) of the GDPR, the controller shall take into account […] the state of the art, the implementation costs, as well as the nature, scope, context and processing purposes and the risks of varying likelihood and severity to the rights and freedoms of persons, appropriate technical and organizational measures to ensure an appropriate level of security […].

Pursuant to the second paragraph of Article 32, when assessing the appropriate security level, taking into account the processing risks, in particular as a result of the destruction, loss, modification or unauthorized disclosure of or access to any transmitted, stored or otherwise processed data, whether accidentally or unlawfully.

2.4 Administrative fine

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

the

AVG and Article 14, third paragraph, of the UAVG, the AP is authorized to file a complaint with regard to infringements of the AVG.

administrative fine.

2.4.1 GDPR

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

administrative fines imposed under this Article for the items referred to in paragraphs four, five

and six listed breaches of this Regulation are effective, proportionate and dissuasive in each case.

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

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

It follows from the fourth paragraph, opening words and under a, that an infringement of the obligations of the

controller and processor as per Article 32 of the GDPR in accordance with paragraph 2

Date

March 24, 2020

Our reference

[CONFIDENTIAL]

is subject to an administrative 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.

It follows from the fifth paragraph, opening words and under a, that an infringement of the basic principles regarding processing as in

Article 9 of the GDPR pursuant to paragraph 2 is subject to an administrative fine of up to

€20,000,000 or, for a company, up to 4% of total worldwide annual sales in the previous

financial year, if this figure is higher.

2.4.2 UAVG

Pursuant to Article 14, paragraph 3, of the UAVG, the AP may, in the event of a violation of the provisions of Article 83, fourth, fifth or sixth paragraph, of the Regulation, impose an administrative fine not exceeding the in amounts referred to in these members.

3. Facts

-

The AP has established that CP&A will in any case from March 12, 2019 to May 2, 2019 absenteeism records in a Google Drive file on the Internet that contains the following data of 25 (sick) employees were listed1:

-

branch;

- Name;

- Last name;

- Starting date;

-

End date;

- Number of calendar days;

- grounds for absence;

-

- social security number;

- Date of birth;

- Employment

(temporary/permanent);

- Date service;

- Contractures;

-

- Comments;

-

- House number;

-

- Residence;

-

Prognosis

(short/medium/long);

End of contract date.

Phone number;

(nursing) address;

E-mail address;

Postal Code;

In this period from March 12 to May 2, 2019, the AP via the web address known to it has the

website six times and found to be without any authentication or other

access control could view the absence registration. The AP has further determined that the

absence registration has been actively updated due to the fact that the contents of the absence registration

changed weekly.2

By letter dated 7 May 2019, CP&A indicated that the relevant file with

health data has been removed and is no longer available.3 The AP determined on May 13, 2019

that the absence registration was no longer accessible via the web address known to it.4 In addition,

1 AP research report, September 3, 2019, appendix 2 to 8.

2 AP research report, September 3, 2019, appendix 2 to 8.

3 Letter of 7 May 2019 from CP&A to the AP.

4 AP research report, September 3, 2019, appendix 8.

Date

the AP determined on the basis of a copy of CP&A's new absence registration that CP&A

no longer registers the reason for absence.5

4.Review

4.1 Processing of health data

As stated in chapter 3, the AP has determined that CP&A in any case from March 12, 2019 to

as of May 2, 2019, maintained an absence record in a Google Drive file in which the following

personal data of 25 (sick) employees were listed: the name, surname,

(nursing) address, house number, zip code, place of residence, telephone number, e-mail address,

Citizen Service Number (BSN) and date of birth.6 This meant that the CP&A employees involved were immediately

identifiable. The aforementioned data are therefore personal data as referred to in Article 4,

part 1 of the GDPR.

Furthermore, the AP has established that CP&A in the absenteeism registration provides the reason for absence (about both

the physical and

as mental health), the prognosis and the comments about the reason for absence and prognosis about this

employees.7 In the opinion of the AP, these data are health data

within the meaning of Article 4(15) of the GDPR.

By digitally registering, storing, updating and making these personal data available from

(sick) employees and keeping up with the absenteeism registration, CP&A has data about health

(partially) automated processing within the meaning of Article 4, part 2, of the GDPR.

In view of the foregoing, the AP concludes that CP&A data on the health of 25

employees in the period from March 12, 2019 to May 2, 2019.

4.2 Controller

The AP is of the opinion that CP&A has determined the purposes and means for the processing of personal data,

including health data. CP&A has stated that absenteeism and reintegration

is an important point of attention within the organisation. CP&A has made the decision to

to include an overview of its sick employees in a file specially designed for that purpose in order to

to keep an overview, to prevent people from getting out of the picture and to interpret them in the best possible way

can give to the reintegration.8 In addition, the fact that CP&A has the absence registration

removed that the decision-making power of whether or not to process absenteeism data rests with CP&A.

5 Letter dated August 7, 2019 from CP&A to the AP.

6 AP research report, September 3, 2019, appendix 2 to 8.

7 AP research report, September 3, 2019, appendix 2 to 8.

8 Opinion CP&A, 12 November 2019, p. 2.

Date

March 24, 2020

Our reference

[CONFIDENTIAL]

The AP designates CP&A as the controller as referred to in Article 4(7) of the

GDPR.

4.3 Violation of the prohibition on processing health data

4.3.1 Introduction

Health data falls under the special category of personal data.

Personal data that are particularly sensitive deserve specific protection, because the processing

can pose high risks to fundamental rights and freedoms. The processing of

special categories of personal data is therefore, pursuant to Article 9(1) of the GDPR

prohibited, unless a legal exception applies.9

In the following, the AP checks whether CP&A can successfully invoke the relevant criteria for this case:

exception as referred to in Article 9, second paragraph, preamble and under b of the GDPR jo. Article 30, first paragraph,

preamble and under b, of the UAVG.

4.3.2 Legal framework

Pursuant to Article 9, second paragraph, preamble and under b of the GDPR, the controller may process health data if this is necessary for the implementation of obligations and the exercise of specific rights of the controller or the person concerned in the field of labor law and social security and social protection law.

This exception does not apply directly on the basis of the GDPR, but leaves room for the Member States to arrive at a more detailed explanation. That happened in the Netherlands in the UAVG.

Article 30, first paragraph, preamble and under b of the UAVG provides in that context that the processing of data about health is allowed if this is necessary for the reintegration or guidance of employees or benefit claimants in connection with illness or incapacity for work. In sector-specific legislation, this ground for exception is then specified in more detail. With regard to reintegration, the AP notes that employers are obliged, pursuant to Article 658a, second paragraph, of Book 7 of the Civil Code (BW) to take those measures as soon as possible that are necessary to enable a sick employee to to do his own or other appropriate work. Although processing of health data may therefore be mandatory, the nature and scope of the data that may be processed is limited by the requirement of necessity as laid down in Article 9, second paragraph, preamble, and under b, GDPR. This means that there must always be an assessment of each processing whether the processing is really necessary in light of the reintegration obligation that rests on the employer.

In the policy rules 'The sick employee' (the policy rules) of the AP, which was published on 29 April 2016 in the Government Gazette, it is specified which medical personal data the employer in the within the framework of reintegration and absenteeism counseling may be processed and can be used as necessary

9 See also Recital 51 of the GDPR.

Date

March 24, 2020

which are not necessary and therefore may not be processed.10 The legal rules
regarding the processing of personal data about the health of sick employees in the context of
their reintegration and absenteeism guidance as laid down in the Protection Act
personal data has not changed with the GDPR coming into effect on 25 May 2018.11 The
policy rules, although written in the context of the Wbp, are therefore still of corresponding
applicable to processing operations under the GDPR.

The data that may be processed according to these policy rules are:12

- the work for which the employee is no longer or is still capable (functional)
limitations, residual opportunities and implications for the type of work the employee can still do
to do);
- the expected duration of the absence;
- the extent to which the employee is incapacitated for work (based on functional limitations,
-
residual possibilities and implications for the type of work the employee can still do);
any advice on adjustments, work facilities or interventions that the employer
the reintegration has to take place.

The data that may not be processed under these policies include:13

- diagnoses, name of illness, specific complaints or indications of pain;
-
-
- other situational problems, such as relationship problems, past problems, relocation,
own subjective observations, both about mental and physical health;
data about therapies, appointments with doctors, physiotherapists, psychologists, etc.;
death of partner, divorce, etc.

4.3.3 Assessment

As stated in chapter 3, the AP established that CP&A kept an absence registration in which the reason for absenteeism (on both physical and mental health), the prognosis and comments on the reason for absenteeism and the prognosis for its employees was recorded.

The AP has assessed this data on the basis of the aforementioned legal framework. In the policy rules of the AP, it has been specified which medical personal data the employer can provide in the context of the reintegration and absenteeism guidance and can be used as necessary designated. The AP concludes that the absenteeism registration contained health data which, due to the lack of a necessity, were not allowed to be processed by CP&A. It's alright in doing so for the reasons for absenteeism stated with regard to 25 involved parties, including the names of physical and mental illnesses, specific complaints and indications of pain. For some employees in the comment box further information is recorded about health.

10 Policy rules for the processing of personal data about the health of sick employees, Dutch Data Protection Authority (Government Gazette 2016, 21703).

11 See the old Article 21, first paragraph, opening words and under f, under 2, of the Personal Data Protection Act and the current Article 30, first paragraph, under b, of the UAVG. And Parliamentary Papers II 2017/2018, 34851, 3, p. 109.

12 Policy rules sick employee, paragraph 5.2.2., p. 27.

13 Policy rules sick employee, paragraph 5.2.1., p. 25, read in conjunction with p. 27.

Pursuant to Article 9, second paragraph, preamble and under b of the GDPR, the controller may process health data if this is necessary for the implementation of

obligations and the exercise of specific rights of the controller or the

person concerned in the field of labor law and social security and social protection law.

Article 30, first paragraph, preamble and under b of the UAVG provides in that context that the processing of data

about health is allowed if this is necessary for the reintegration or guidance of employees

or benefit claimants in connection with illness or incapacity for work. Because processing

names of diseases, specific complaints and indications of pain is not necessary for the reintegration of

employees, as also follows the policies of the AP, their processing is prohibited. CP&A can

thus not successfully invoking Article 30, first paragraph and under b, of the UAVG. The AP has not been found

that CP&A can successfully invoke the other exceptions of Article 30 of the UAVG. the AP

thus, CP&A believes that the above-mentioned health data violates the prohibition of Article

9, first paragraph, of the GDPR.

With regard to the period of this violation, the AP last determined on May 2, 2019 that

CP&A has processed the health data in its absenteeism registration. As mentioned in chapter 3

the AP subsequently established on 13 May 2019 that the absence registration is no longer accessible via

the web address known to her. Finally, the AP has established that in the current absenteeism registration the

reason for absence is no longer registered by CP&A.

4.3.4 Conclusion

The AP comes to the conclusion that CP&A, as a data controller, has been notified of at least March 12, 2019

up to and including 2 May 2019, has violated the prohibition of Article 9(1) of the GDPR by

to process health data of 25 employees.

4.4 Processing Security Violation

4.4.1 Introduction

To ensure security and prevent the processing of personal data from infringing

to the GDPR, the controller must, pursuant to Article 32 of the GDPR,

processing inherent risks and take measures to mitigate risks. That

measures should ensure an appropriate level of security, taking into account the status

of the technology and the implementation costs compared to the risks and the nature of the

personal data.14 In the following, the AP checks whether CP&A has an appropriate security level

used for the processing of the health data in its absenteeism registration as

accessible via the web address.

4.4.2 Assessment

Pursuant to Article 32(1) of the GDPR, the controller must provide appropriate and

take technical and organizational measures to ensure a security level appropriate to the risk

14 Recital 83 of the GDPR.

Date

March 24, 2020

Our reference

[CONFIDENTIAL]

to ensure. In assessing the risks, according to Article 32, second paragraph, of the GDPR, attention must be paid to

to be spent on risks that arise in the processing of personal data, such as the

unauthorized disclosure or access to the transmitted, stored or

otherwise processed data, either accidentally or unlawfully.

The more sensitive the data is, or the context in which it is used a

poses a greater threat to the privacy of those involved, stricter requirements are imposed

placed on data security. This means that high demands are made on the technical and

organizational measures to protect this data.15 With regard to authentication at the

access to the processing of data about the health of (sick) employees and where access

is provided via the internet, one must therefore take stricter measures to comply with a

appropriate security level, such as two-factor authentication.16

The AP has established that the absenteeism registration (containing health data) of CP&A without

some form of authentication was accessible. The AP is of the opinion that CP&A vis-à-vis its

absenteeism registration has applied an insufficiently appropriate security level. CP&A had seen the
sensitive nature of the data, the fact that the health data was processed on the internet and
the risks to the privacy of the data subjects should take further measures to prevent the
mitigate the risk of unauthorized access to the absence registration. However, CP&A has failed to do so.
She could have avoided this lack of security by, for example,
implement an authentication technique (or other method) to verify the claimed identity of a
user of the absenteeism registration. The AP considers such a security measure,
appropriate in view of the current state of the art and implementation costs.
The AP is therefore of the opinion that CP&A has violated Article 32, first paragraph, of the GDPR because CP&A
an insufficiently appropriate in relation to the health data in its absenteeism registration
security level.

CP&A view and AP response

CP&A argues in its view that it had only one aim with the absenteeism registration: to
support employees as best as possible during a period of illness and reintegration. CP&A
believed that it handled it correctly, in accordance with the applicable regulations
with the data of the employees involved and also carefully had that data in such a way
secured that they were not freely accessible. To protect the privacy of the data subject
employees, the file was only accessible via a specific link. The link was only provided to
those persons who are/were involved in the reintegration of employees and as such
absenteeism data had to be available to guide the employees as well as possible
absenteeism and reintegration (management, two regional managers, one HRM employee, the HRM
manager and the absenteeism supervisor). Other than those people, no one had access. CP&A doesn't have one
take into account that the link would be provided to a third party without authorization. With today's knowledge

15 See also Policy rules for the processing of personal data about the health of sick employees, p. 13.

16 See also policy rules for the processing of personal data about the health of sick employees, p. 7.

Date

March 24, 2020

Our reference

[CONFIDENTIAL]

CP&A deeply regrets that it did not see that risk and that it therefore reduced it for a third

possible to consult the data.

Based on CP&A's view, the AP does not come to a different conclusion. Providing a

specific link only to persons who are/were involved in the reintegration of employees

albeit an organizational measure that benefits the security of personal data.

However, given the sensitive nature of the data, CP&A had the health data on the

internet were processed and the risks to the privacy of those involved also a

appropriate technical measure, such as, for example, the implementation of a

authentication technique at the link. With such a measure, CP&A had the risk that a third party

unauthorized access to highly sensitive data.

4.4.3 Conclusion

The AP comes to the conclusion that CP&A, as a data controller, has been notified of at least March 12, 2019

up to and including 2 May 2019, has infringed Article 32(1) of the GDPR by

health data in its absenteeism registration to use an insufficiently appropriate security level.

4.5 Final conclusion

First of all, the AP comes to the conclusion that CP&A from at least March 12, 2019 to May 2, 2019

has violated the prohibition of Article 9(1) of the GDPR by health data of 25

processing employees. In addition, the AP comes to the conclusion that CP&A in the same period

32, first paragraph, of the GDPR by having regard to this health data in its

absenteeism registration does not take adequate technical and organizational measures to

to ensure a level of security appropriate to the risk.

5. Fine

5.1 Introduction

From at least March 12, 2019 to May 2, 2019, CP&A has Article 9, first paragraph, and Article 32, first paragraph of the GDPR. With regard to both established violations, the AP uses of its authority to impose a fine on CP&A pursuant to Article 58, second paragraph, preamble and under i and Article 83, paragraphs 4 and 5, of the GDPR read in conjunction with Article 14, paragraph 3, of the UAVG. For this, the AP uses the Fine Policy Rules 2019.17

In the following, the AP will first briefly explain the fine system, followed by the motivation of the amount of the fine in the present cases.

17 Stct. 2019, 14586, March 14, 2019.

5.2 Fines Policy Rules of the Dutch Data Protection Authority 2019 (Fines Policy Rules 2019)

In the event of a violation of the unlawful processing of special personal data pursuant to Article 9, first paragraph, of the GDPR, the AP is authorized to impose a fine up to a maximum of € 20,000,000, or up to 4% of the total worldwide annual turnover in the previous financial year, whichever is higher. This based on article 58, second paragraph, preamble and under i and Article 83 of the GDPR read in conjunction with Article 14, third paragraph, of the UAVG. On the basis of the appendix to the Fine Policy Rules 2019, this violation falls within the highest category, namely category IV.

And for violation of Article 32, first paragraph, of the GDPR, the AP is authorized to impose an administrative fine up to € 10,000,000 or up to 2% of the total worldwide annual turnover in the previous financial year, if this figure is higher. Based on the appendix to the Fine Policy Rules 2019, this violation falls into category II.

On the basis of Article 2.3 of the Fine Policy Rules 2019, the AP applies for the above

violations the following penalty bandwidths:

Category II: Fine range between €120,000 and €500,000 and a basic fine of €310,000. […].

Category IV: Fine range between €450,000 and €1,000,000 and a basic fine of €725,000. […].

Pursuant to Article 6 of the Fine Policy Rules 2019, the AP determines the amount of the fine by dividing the amount from the basic fine upwards (up to a maximum of the bandwidth of the violation linked fine category) or down (to at least the minimum of that bandwidth). The basic fine is increased or decreased depending on the extent to which the factors referred to in Article 7 of the 2019 Fine Policy Rules give rise to this.

Pursuant to Article 7, without prejudice to Articles 3:4 and 5:46 of the General Administrative Law Act (Awb) taking into account the factors derived from Article 83, second paragraph, of the GDPR and in the Policy rules 2019 referred to under a to k:

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

b. the intentional or negligent nature of the infringement;

c. the measures taken by the controller […] to address the data subjects suffered limit damage;

d. the extent to which the controller […] is responsible given the technical and organizational measures that he has carried out in accordance with Articles 25 and 32 of the GDPR;

e. previous relevant breaches by the controller […];

f. the extent to which there has been cooperation with the supervisory authority to remedy the breach 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 […] has notified the breach;

i. compliance with the measures referred to in Article 58, paragraph 2, of the GDPR, insofar as they are previously

with regard to the controller […] in question with regard to the same

Date

March 24, 2020

Our reference

[CONFIDENTIAL]

matter have been taken;

j. adherence to approved codes of conduct in accordance with Article 40 of the GDPR or of

approved certification mechanisms in accordance with Article 42 of the GDPR; and

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

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

result.

In the present case, it concerns an assessment of the nature, seriousness and duration of the violation

in the specific case. In principle, within the bandwidth of the violation

linked fine category. The AP may, if necessary and depending on the extent to which the aforementioned

factors give rise to this, on the basis of Article 8.1 of the Fines Policy Rules 2019 de

apply penalty bandwidth of the next higher and next lower category respectively. In addition

the AP assesses when imposing an administrative fine on the basis of Article 5:46, second paragraph, of the

Awb to what extent this can be blamed on the offender. Finally, the AP will, on the basis of its

Fines policy rules 2019 and articles 3:4 and 5:46 of the Awb assess whether the application of its policy for

determining the amount of the fine, given the circumstances and the capacity of CP&A in this

specific case, does not lead to a disproportionate outcome.

5.3 Fine for violation of the prohibition on processing data about health and health

processing security

5.3.1. Nature, seriousness and duration of the infringement

Pursuant to Article 7, opening words and under a, of the Fine Policy Rules 2019, the AP takes into account the nature,

the seriousness and duration of the infringement. In its assessment, the AP takes into account, among other things, the nature, the
scope or purpose of the processing as well as the number of data subjects affected and the scope of the data suffered damage to them.

The protection of natural persons with regard to the processing of personal data is a fundamental right. Under Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16, paragraph 1 of the Treaty on the Functioning of the European Union (TFEU), everyone has the right to protection of his personal data. The principles and rules concerning the protection of natural persons when processing their personal data must be in accordance with their fundamental rights and freedoms, in particular their right to protection of personal data. The GDPR aims to contribute to the creation of an area of freedom, security and justice and of economic union, as well as to economic and social progress, the strengthening and convergence of economies within the internal market and the well-being of natural persons. The processing of personal data must serve people. The right to protection of personal data is not absolute, but must be considered in relation to to its function in society and must conform to the principle of proportionality against other fundamental rights are weighed up. Any processing of personal data must be fair and lawful to happen. The personal data must be sufficient, relevant and limited to: what is necessary for the purposes for which they are processed. Personal data must be

processed in a manner that ensures appropriate security and confidentiality of that data, also to prevent unauthorized access to or use of personal data and

the equipment used for processing.

The GDPR offers a high level of protection for particularly sensitive personal data.

Personal data that are particularly sensitive deserve specific protection, because the processing can pose high risks to fundamental rights and freedoms. Those involved serve therefore have a high degree of control over their health data. The starting point is therefore that processing of special personal data is in principle prohibited. There is only a limited number of and exceptions laid down in the (U) AVG are possible. CP&A has with the processing of health data in this case the high level of protection offered by Article 9(1) of the GDPR violated.

Pursuant to Article 32(1) of the GDPR, the controller must also:

take appropriate technical and organizational measures to ensure a risk-adjusted to ensure a level of security. In determining the risk to the data subject, the nature of the personal data and the nature of the processing of interest: these factors determine the potential damage to the individual data subject in the event of, for example, loss, alteration or unlawful processing the data. The AP has come to the conclusion that CP&A is not an appropriate has taken security measures that relate to the health data in its absenteeism registration.

The AP has determined that CP&A from at least March 12, 2019 to May 2, 2019 processed health data of 25 employees without appropriate security. This one health data contained highly sensitive information such as names of physical and mental illnesses, specific complaints and pain indications of its employees. During this period, CP&A has have violated the prohibition on the processing of special personal data and have data subjects therefore had no control over their health data. And it is precisely this control that the GDPR wants to offer to data subjects, so that data subjects are able to protect their personal data and to surrender it freely. In addition, during this period, the absenteeism registration of CP&A accessible without any form of authentication. This gives CP&A employees a high and unnecessary risk of unauthorized access to their personal data. The fact that it's here

concerns the processing of particularly sensitive data, an insufficient security of the

data extra.

In the opinion of the AP, there are therefore two serious violations in which CP&A

has processed data of data subjects under incorrect conditions, but pursuant to Article 7

of the Fines Policy Rules 2019 to the extent applicable in the present

case there is no reason to increase or decrease the amount of the fine. However, in paragraph 5.4, the AP will

assess whether the amount of the fine needs to be adjusted on the basis of proportionality.

5.3.2 Blame

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

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

violations, the imposition of an administrative fine in accordance with established case law18 does not require that

it is demonstrated that there is intent and the AP may presume culpability if it

offense is established.19

Pursuant to Article 9(1) of the GDPR, it is in principle prohibited to disclose health data

to process. The legal rules regarding the processing of personal data about the health of

sick employees in the context of their reintegration and absenteeism guidance as laid down in

the Personal Data Protection Act with the GDPR coming into effect on May 25, 2018

not changed. In addition, CP&A had from the policy rules 'The sick employee' of the AP, which had already been published on

29

have been published in the Government Gazette in April 2016, can determine which personal data CP&A does and

should not have processed. A party such as CP&A may, partly in view of the special nature of the

personal data, are expected to duly ascertain the standards that apply to it and
comply with this. CP&A has a high level of protection for special
personal data violated. The AP considers this to be culpable.
Pursuant to Article 32 of the GDPR, the policy rules 'The sick employee' and the nature of the processing,
CP&A should also have known that it should have taken further measures to reduce the risk of
to mitigate unauthorized access to the absence registration. CP&A has failed to provide access to
the absence registration via the web address in any case uses a suitable authentication technique (or another
method) to prove a user's claimed identity. Also this
considers the AP culpable.
5.3.3 CP&A opinion and AP . response
CP&A states in its view that it has taken the corrective measures already taken,
which she understands to the AP refers to the request of the AP to rectify the violation as soon as possible
terminate, and has immediately provided full cooperation. The absence registration will only be
maintained in the secure environment of the HRM system, which is only accessible to the department
HRM and direct managers. In addition, CP&A no longer processes the reason for absence and the
prognosis only registered insofar as it can be deduced from the reports of the company doctor
without medical information.
In view of the foregoing and thereby also expressly taking into account the fact that CP&A is a
is a medium-sized enterprise within the meaning of Article 2a UAVG and taking into account the way in which
for example, the issues of Nippon Express (2017) and Stichting Abtona (2016) have been resolved
CP&A the AP to suffice with the corrective measures already taken pursuant to Article 58 of the GDPR.
In addition, CP&A points to the fact that the parties concerned — fortunately — were not harmed, that
CP&A has in no way acted intentionally or negligently, that there have been no previous infringements
and that CP&A has deployed (additional) guidance from an external advisor in the field of privacy.
18 Cf. CBb 29 October 2014, ECLI:NL:CBB:2014:395, r.o. 3.5.4, CBb September 2, 2015, ECLI:NL:CBB:2015:312, r.o. 3.7
and CBb March 7, 2016,

ECLI:NL:CBB:2016:54, r.o. 8.3, ABRvS 29 August 2018, ECLI:NL:RVS:2018:2879, r.o. 3.2 and ABRvS December 5, 2018, ECLI:NL:RVS:2018:3969, r.o. 5.1.

19 Parliamentary Papers II 2003/04, 29702, no. 3, p. 134.

Date

March 24, 2020

Our reference

[CONFIDENTIAL]

The AP does not share CP&A's view. CP&A should have failed to provide health data in this case of its employees. In addition, CP&A has not taken adequate measures to ensure the security of its absenteeism system. This CP&A conduct is detrimental committed to protecting the personal data of its employees. Given the seriousness of the violations, the AP considers the imposition of a corrective measure, other than an administrative fine, insufficiently effective, proportionate and dissuasive. The AP finds the imposition of an administrative fine appropriate in this case. In determining the height, it will take into account the position and capacity of CP&A. CP&A has also stated that the data subjects are not harm caused, but this has not been proven, nor can it be ruled out that further damage may occur in the future to arise. This ground of appeal, alone or together with the other complaints, is given by the AP in view of the seriousness of the violations and the degree of culpability are no reason to refrain from imposing a fine or further mitigate the fine on the grounds stated by CP&A.

The AP sets the fine for violation of Article 9, first paragraph, of the GDPR at € 725,000. And for the violation of Article 32, first paragraph, of the GDPR, the AP sets the fine at € 310,000.

5.4 Proportionality and capacity

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

inter alia play in the accumulation of sanctions and the capacity of the

controller.

CP&A has invoked limited capacity. Based on the at the AP at the moment

known financial data from CP&A, the AP considers the capacity of CP&A to be limited, as a result of which the AP to

the conclusion is that CP&A will pay the combined fine of both violations of €1,035,000

cannot afford it financially. On this basis, the AP sees reason to reduce the fine. the AP

deems a fine of € 15,000 appropriate and appropriate in this case and deems CP&A to have sufficient financial means to

to pay this amount.

5.5 Conclusion

The AP sets the total fine at € 15,000.

6.Dictum

fine

The AP submits to CP&A, for violation of Article 9, first paragraph, of the GDPR and Article 32, first paragraph, of

the GDPR imposes an administrative fine in the amount of € 15,000 (in words: fifteen thousand euros).20

Yours faithfully,

Authority Personal Data,

w.g.

drs. C.E. Mur

board member

Remedies Clause

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

decide to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority. Submit it of a notice of objection suspends the effect of this decision. For submitting a digital objection, see www.autoriteitpersoonsgegevens.nl, under the heading Objecting to a decision, at the bottom of the page under the heading Contact with the Dutch Data Protection Authority. The address for paper submission is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague.

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

In your notice of objection, write at least:

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

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