Confidential/Registered

CP&A B.V.

Attn. the direction

PO Box 514

5600 AM Eindhoven

Date

March 24, 2020

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 management,

The Dutch Data Protection Authority (AP) has decided to CP&A B.V. (CP&A) an administrative fine of

€ 15,000 to be imposed. The AP is of the opinion that from March 12, 2019 to May 2, 2019, CP&A

of Article 9, paragraph 1, 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 insufficiently appropriate security measures have been taken if

referred to in Article 32, first paragraph, 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 AP assesses whether there are any processing of health data, the controller's responsibility and the violations. In Chapter 5 details 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 excerpt from the commercial register, has approximately 160 employees. CP&A performed according to the trade register and its website, among other things, inspection and maintenance work of public objects.

On January 11, 2019, the AP received a notification that CP&A is processing health data from it employees. From the report, supervisors of the AP concluded that CP&A had an online maintains absenteeism registration containing health data of sick employees. As a result of this signal, the AP has started an (ex officio) investigation into compliance by CP&A with Articles 9 and 32 of the GDPR.

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

guarantees, as referred to in Article 32, first paragraph, of the GDPR.

1.2 Process flow

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

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

violation as soon as possible. On May 2, 2019, the AP, in response to the telephone

sent a standard-conveying letter and the legal framework with regard to the notification obligation of

breaches in connection with personal data explained to the AP. By letter dated May 7, 2019, CP&A notified the

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

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

personal data.

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

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

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

In a letter dated October 30, 2019, the AP informed CP&A of its intention to enforce and to

basic investigation report sent and CP&A was given the opportunity to do so

express point of view. On November 12, 2019, CP&A issued a written opinion

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

opportunity to respond to these documents. CP&A has not used it.

2. Legal framework

2.1 Scope GDPR

Pursuant to Article 2, paragraph 1, of the GDPR, this Regulation applies to the whole or in part

automated processing, as well as to the processing of personal data contained in a file included or intended to be included therein.

Pursuant to Article 3, paragraph 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 takes place 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 relating to 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”: a […] legal entity that, alone or jointly with others, achieves the purpose of and determines 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 related to the physical or mental health of a natural person, including data about health services provided that provide information about his state of health.

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

Exceptions to the prohibition on processing sensitive personal data are stated in Article 9, second paragraph of the GDPR. Insofar 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 the data subject in relation to it labor law and social security and social protection law, to the extent permitted by Union law or Member State law or by collective agreement based on Member State law provides appropriate safeguards for the fundamental rights and interests of the data subject;

Date

March 24, 2020

Our reference

[CONFIDENTIAL]

[…]

In accordance with Article 30 of the General Data Protection Regulation Implementation Act (UAVG), attention has been paid to

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 that work 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 disability.

[…]

2.3 Security of Processing

Pursuant to Article 32, paragraph 1, of the GDPR, the controller shall take […], taking into account with the state of the art, the implementation costs, as well as with the nature, size, context and the processing purposes and the varying likelihood and severity of risks to the rights and liberties of persons, appropriate technical and organizational measures to prevent one at risk to ensure an appropriate level of security […].

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

2.4 Administrative fine

Pursuant to Article 58, paragraph 2, opening words and under i, in conjunction with Article 83, paragraphs 4 and 5, of the GDPR and Article 14, third paragraph, of the UAVG, the AP is authorized to take a impose an administrative fine.

2.4.1 GDPR

Pursuant to Article 83, paragraph 1, of the GDPR, each supervisory authority ensures that the administrative fines imposed under this Article for the offenses referred to in paragraphs four, five and six reported infringements of this Regulation are effective, proportionate and dissuasive in each case.

Pursuant to paragraph 2, administrative fines shall be imposed, depending on the circumstances of the specific case, imposed in addition to or instead of the provisions referred to in Article 58, paragraph 2, under a to h and under j, referred measures.

It follows from the fourth paragraph, preamble and under a, that a breach of the obligations of the controller and the processor as in Article 32 of the GDPR in accordance with paragraph 2

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, if this figure is higher.

It follows from the fifth paragraph, preamble and under a, that an infringement of the basic principles regarding processing as in Article 9 of the GDPR is subject to an administrative fine up to €20,000,000 or, for a company, up to 4% of total worldwide annual turnover in the previous financial year, if this figure is higher.

2.4.2 UAVG

Pursuant to Article 14, third paragraph, 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 bye-law impose an administrative fine of at most the in

amounts mentioned in these paragraphs.

3. Facts

-

The AP has determined that CP&A will in any event from March 12, 2019 up to and including May 2, 2019

absentee registration in a Google Drive file on the Internet in which the following

details of 25 (sick) employees were listed1:

-

branch;

- Name;

- Last name;

- Starting date;

-

End date;

- Number of calendar days;

- Reason for absenteeism;

-

- citizen service number;

- Date of birth;

- Employment

(temporary/permanent);

- Date service;

- Contract hours;

-

- 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 has used the web address known to it to

visited website six times and found it without any kind of authentication or other

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

absence registration was actively updated due to the fact that the contents of the absence registration

changed weekly.2

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

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

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

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

2 AP research report, 3 September 2019, appendices 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

March 24, 2020

the DPA determined on the basis of a copy of CP&A's new absenteeism registration that CP&A has the

reason for absence is no longer registered.5

4.Assessment

4.1 Processing of Health Data

As stated in Chapter 3, the AP has determined that CP&A will in any event from March 12, 2019 until

with May 2, 2019 maintained an absence record in a Google Drive file that includes the following

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

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

BSN, and the date of birth.6 The CP&A employees involved were immediately aware of this

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

part 1 of the GDPR.

The AP has also established that CP&A has included the reason for absenteeism (both physical and physical) in the absence

registration

as mental health), the prognosis and the comments on 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 available this personal data

(sick) employees and keeping track of the absence registration, CP&A has data about health

(partially) automatically processed 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 through May 2, 2019.

4.2 Controller

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

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

is an important focus within the organization. CP&A has made the decision to launch a

to include an overview of its sick employees in a specially designed file to keep it

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

can give to the reintegration.8 In addition, it is apparent from the fact that CP&A has the absenteeism registration

removed that the decision whether or not to process absence data rests with CP&A.

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

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

7 AP research report, 3 September 2019, appendices 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, part 7, of the

AVG.

4.3 Violation of the Prohibition of Processing Health Data

4.3.1 Introduction

Health data fall 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 based on Article 9, first paragraph, of the GDPR

prohibited unless a legal exception applies.9

In the following, the AP assesses whether CP&A can successfully invoke the relevant provisions for this case

exception as referred to in Article 9, paragraph 2, opening lines and under b of the GDPR jo. article 30, paragraph 1,

preamble and under b of the UAVG.

4.3.2 Legal framework

Pursuant to Article 9, paragraph 2, opening lines 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 involved 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 Member States to arrive at a more detailed definition. This happened in the Netherlands in the UAVG.

Article 30, first paragraph, preamble and under b of the UAVG stipulates in that context that the processing of data about health is allowed if this is necessary for the reintegration or guidance of employees or beneficiaries in connection with illness or incapacity for work. In sector-specific legislation this ground for exception is then specified in more detail. The AP notes with regard to reintegration that employers are obliged, pursuant to Article 658a, second paragraph, of Book 7 of the Civil Code (BW) to take the necessary measures as soon as possible to enable a sick employee to do his own or other appropriate work. Although processing of health data than therefore may be mandatory, the nature and scope of the data that may be processed does limited by the requirement of necessity as laid down in Article 9, second paragraph, opening words, and under b, AVG. This means that an assessment of each processing must always take place whether the processing is also really necessary in the 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 April 29, 2016 in the Government Gazette, it has been specified which medical personal data the employer has in it within the framework of the reintegration and absenteeism guidance may be processed and considered necessary

9 See also recital 51 of the GDPR.

Date

March 24, 2020

Our reference

labeled, and which are not necessary and may therefore not be processed.10 The statutory 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 becoming applicable on 25 May 2018.11 The policy rules, although written in the context of the Wbp, are therefore still equivalent applicable to processing operations under the GDPR.

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

- the activities that the employee is no longer or still capable of (functional limitations, residual possibilities and implications for the type of work that the employee can still do doing);
- 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 adaptations, work facilities or interventions that the employer provides the reintegration must take place.

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

- diagnoses, disease name, specific complaints or indications of pain;
-
-
- other situational problems, such as relationship problems, problems from the past, relocation, own subjective perceptions, both about mental and physical health status;

information about therapies, appointments with doctors, physiotherapists, psychologists, etc.;

partner's death, divorce, etc.

4.3.3 Assessment

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

The AP has assessed this data on the basis of the aforementioned legal framework. In the The policy rules of the AP specify which medical personal data the employer uses in the context of the reintegration and absenteeism guidance may process and be deemed necessary marked. The AP comes to the conclusion that the absence registration contained data about health which, for lack of necessity, were not allowed to be processed by CP&A. It's alright in addition to the reasons for absenteeism stated with regard to 25 persons involved, including names of physical and mental illnesses, specific complaints and indications of pain. For some employees, it is remarks field further information recorded about health.

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

11 See the old article 21, first paragraph, opening lines 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 Documents II 2017/2018, 34851, 3, p. 109.

12 Policy rules for sick employees, paragraph 5.2.2., p. 27.

13 Sick employee policy rules, paragraph 5.2.1., p. 25, read in conjunction with p. 27.

Date

March 24, 2020

Our reference

[CONFIDENTIAL]

Pursuant to Article 9, paragraph 2, opening lines 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 involved in the field of labor law and social security and social protection law.

Article 30, first paragraph, preamble and under b of the UAVG stipulates in that context that the processing of data about health is allowed if this is necessary for the reintegration or guidance of employees or beneficiaries in connection with illness or incapacity for work. Because processing names of illnesses, specific complaints and indications of pain is not necessary for the reintegration of employees, as also follows from the policy rules of the AP, the processing thereof is prohibited. CP&A can thus cannot successfully invoke article 30, first paragraph and under b, of the UAVG. The AP has not turned up that CP&A can successfully invoke the other exceptions of Article 30 of the UAVG. The AP therefore considers that CP&A's above health data violates the prohibition of Art 9, first paragraph, of the GDPR.

With regard to the period of this violation, the AP last determined that on May 2, 2019 CP&A has processed the health data in its absence registration. As mentioned in chapter 3 The AP then determined on May 13, 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 controller of at least March 12, 2019 up to and including 2 May 2019, has violated the prohibition of Article 9, first paragraph, 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 being infringed to the GDPR, the controller must, pursuant to Article 32 of the GDPR, provide the assess inherent risks and take measures to mitigate risks. That measures must ensure an appropriate level of security, taking into account the state of the technique and the implementation costs compared to the risks and the nature of the protection

personal data.14 In the following, the AP assesses whether CP&A has an appropriate level of security used for the processing of the health data in its absence registration such as that was accessible via the web address.

4.4.2 Assessment

Pursuant to Article 32, paragraph 1, of the GDPR, the controller must provide appropriate and take technical and organizational measures to ensure a level of security appropriate to the risk

14 Recital 83 of the GDPR.

to ensure. According to Article 32, second paragraph, of the GDPR, attention should be paid to the assessment of the risks to be spent on risks that arise in the processing of personal data, such as the unauthorized disclosure of or unauthorized access to the transmitted, stored or otherwise processed data, whether accidentally or unlawfully.

The more sensitive the data is, the more the context in which it is used poses a greater threat to the privacy of those involved, stricter requirements will be imposed to 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, stricter measures must therefore be taken to comply with a appropriate level of security, such as two-factor authentication.16

The AP has determined that the absence registration (containing health data) of CP&A without some form of authentication was accessible. The AP is of the opinion that CP&A absence 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 must take further measures to prevent it
mitigate the risk of unauthorized access to the absence registration. However, CP&A failed to do so.
She could have avoided this lack of security by, for example, using a suitable
implement an authentication technique (or other method) to verify the claimed identity of a
user of the absence registration. The AP deems such a security measure,
appropriate given 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
in relation to the health data in her absence registration an insufficiently appropriate
security level used.

Opinion CP&A and response AP

In its view, CP&A argues that it had only one objective with the absenteeism registration: her
assisting employees as well as possible during a period of illness and reintegration. CP&A
believed that it acted correctly, in accordance with the applicable regulations
with the data of the employees involved and also had that data carefully 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 in order to guide the employees as well as possible
in the case of 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
taken 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 on the health of sick employees, p. 13.

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

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

it has been possible to consult the data.

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

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

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

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

processed over the internet and the risks to the privacy of the data subjects are also a

take appropriate technical measure, such as the implementation of a

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

could gain unauthorized access to highly sensitive data.

4.4.3 Conclusion

The AP comes to the conclusion that CP&A as controller of at least March 12, 2019

up to and including 2 May 2019, has violated article 32, first paragraph, of the GDPR by

health data in its absence registration to maintain an insufficiently appropriate security level.

4.5 Final conclusion

The AP first of all concludes that from at least March 12, 2019 to May 2, 2019, CP&A

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

processing employees. In addition, the AP comes to the conclusion that CP&A article

32, paragraph 1, of the GDPR by regarding this health data in her

absenteeism registration does not take sufficient appropriate technical and organizational measures to prevent a

level of security appropriate to the risk.

5. Fine

5.1 Introduction

From at least March 12, 2019 up to and including May 2, 2019, CP&A has Article 9, first paragraph, and Article 32, first paragraph of the GDPR. The AP makes use of both established violations of its authority to impose a fine on CP&A pursuant to section 58, subsection 2, opening lines and under i and Article 83, fourth and fifth paragraph, of the GDPR read in conjunction with Article 14, third paragraph, of the UAVG. The AP applies the Fining Policy Rules 2019.17 for this

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

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

5.2 Fining Policy Rules of the Dutch Data Protection Authority 2019 (Fining 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 of up to € 20,000,000, or up to 4% of the total worldwide annual turnover in the previous financial year, whichever is higher. This is based on article 58, second paragraph, opening lines and under i and Article 83 of the GDPR read in conjunction with Article 14, third paragraph, of the UAVG. Based on the appendix to the Fining Policy Rules 2019, this violation is the highest category, namely category IV.

And for violation of Article 32, first paragraph, of the AVG, 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 2019 Fining Policy Rules, this violation falls into a category II.

Based on Article 2.3 of the Fining Policy Rules 2019, the AP uses

violations the following penalty ranges:

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 Fining Policy Rules 2019, the AP determines the amount of the fine by the amount from the basic fine upwards (up to a maximum of the bandwidth of the offense linked penalty 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 Fining Policy Rules 2019 give cause to do so.

Pursuant to Article 7, without prejudice to Articles 3:4 and 5:46 of the General Administrative Law Act, the AP (Awb) take 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:

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 harm suffered by them injury;

b. the intentional or negligent nature of the breach;

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

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

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

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, and if so, to what extent, the controller […] has notified the breach;

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

in respect of the controller […] in question in relation 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, which may or may not result directly from the breach

result.

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

in the specific case. In principle, this will be done within the bandwidth of the violation

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

factors give rise to this, pursuant to Article 8.1 of the Fining Policy Rules 2019 de

Apply penalty bandwidth of the next higher or the next lower category respectively. In addition

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

Awb to what extent this can be blamed on the offender. Finally, the AP will be under her

2019 Fining Policy Rules 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 CP&A's capacity in this

specific case, does not lead to a disproportionate outcome.

5.3 Fine amount for violation of prohibition on processing health data and

security of processing

5.3.1. Nature, seriousness and duration of the infringement

Pursuant to Article 7, preamble and under a, of the Fining Policy Rules 2019, the AP takes into account the nature,

the seriousness and duration of the infringement. In assessing this, 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 processing damage suffered to them.

The protection of natural persons with regard to the processing of personal data is a fundamental right. Pursuant to Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16, Everyone has the right to, paragraph 1 of the Treaty on the Functioning of the European Union (TFEU). protection of his personal data. The principles and rules regarding the protection of natural persons when processing their personal data must comply with their fundamental rights and freedoms, in particular their right to protection personal data. The GDPR aims to contribute to the creation of an area of freedom, security and justice and of an 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 its function in society and must, in accordance with the principle of proportionality, against others fundamental rights are considered. Any processing of personal data must be fair and lawful to happen. The personal data must be adequate, 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 the unauthorized use of personal data and

the equipment used for processing.

For particularly sensitive personal data, the GDPR offers a high level of protection.

Personal data that are particularly sensitive deserve specific protection, because the processing can pose high risks to fundamental rights and freedoms. Serving Stakeholders 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 them and exceptions laid down in the (U)GDPR are possible. CP&A has been processing health data in this case the high level of protection that Article 9, first paragraph, of the GDPR offers violated.

Pursuant to Article 32, paragraph 1, of the GDPR, the controller also serves take appropriate and technical and organizational measures to ensure a risk-based approach to ensure a level of security. When determining the risk for the data subject, the nature of the personal data and the nature of the processing are important: these factors determine the potential damage for the individual data subject in the event of loss, alteration or unlawful, for example processing of the data. The AP has come to the conclusion that CP&A is not a suitable has taken security measures that relate to the health data in its absence registration.

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

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

data extra.

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

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

of the Fining Policy Rules 2019 insofar as applicable in the present

case, there is no reason to increase or decrease the fine amount. The AP will, however, in section 5.4

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

5.3.2 Culpability

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. Now this is about

violations, it is not required for the imposition of an administrative fine in accordance with established case law18

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

perpetrator is established.19

Pursuant to Article 9, paragraph 1, of the GDPR, it is in principle prohibited to share 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 will be applicable with the GDPR becoming applicable on 25 May 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

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

should not have processed. Partly in view of the special nature of the

personal data, it is expected that it is duly satisfied with the standards that apply to it
complies with this. Due to its conduct, CP&A has a high level of protection for special
personal data breached. The AP considers this culpable.

Pursuant to Article 32 of the GDPR, the policy rules 'The sick employee' and the nature of the processing had
CP&A should also know that it should have taken further measures to reduce the risk of
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 an appropriate authentication technique (or another
method) to prove the claimed identity of a user. Also this
deems the AP culpable.

5.3.3 CP&A's view and AP's response

In its view, CP&A states that it has taken note of the corrective measures already taken,
which she understands to the AP refers to the AP's request to rectify the violation as soon as possible
terminate, and has immediately provided all cooperation. The absence registration will only become
kept 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 is only registered insofar as it can be derived from the company doctor's reports
without medical information.

In view of the foregoing and 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 manner in which
for example, the issues of Nippon Express (2017) and Stichting Abtona (2016) have been settled requests
CP&A de 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 - fortunately - no damage was caused to those involved, that
CP&A has not acted in any way willfully or negligently, that there have been no prior infringements
and that CP&A has deployed (additional) guidance from an external consultant in the field of privacy.

18 Cf. CBb 29 October 2014, ECLI:NL:CBB:2014:395, r.o. 3.5.4, CBb 2 September 2015, ECLI:NL:CBB:2015:312, r.o. 3.7 and
CBb 7 March 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 sufficient appropriate measures to ensure the security of its absenteeism system. This conduct of CP&A is detrimental done to protect the personal data of its employees. Given the seriousness of the violations, the AP deems the imposition of a corrective measure, other than an administrative fine, insufficiently effective, proportionate and dissuasive. The AP believes that an administrative fine should be imposed appropriate in this case. In doing so, it will take into account the position and strength of CP&A. CP&A has also stated that there is no damage to those involved harmed, but this has not been proven and it cannot be ruled out that further damage may occur in the future to arise. This grievance, alone or together with the other grievances, is given by the AP in view of the seriousness of the violations and the degree of culpability are no reason to waive the imposition of a fine to further moderate the fine on the grounds stated by CP&A.

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

5.4 Proportionality and Capacity

Finally, the AP assesses whether 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. Application of the proportionality principle is possible

play, among other things, 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 CP&A's financial resources to be limited, which means that the AP has to

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

financially unable to bear. On this basis, the AP sees reason to reduce the fine. The AP

considers a fine of € 15,000 appropriate and necessary in this case and deems CP&A to be sufficiently

to pay this amount.

5.5 Conclusion

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

6. Operative part

Fine

The AP will inform CP&A, due to violation of Article 9, first paragraph, of the AVG and Article 32, first paragraph, of

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

Yours faithfully,

Authority for Personal Data,

e.g.

drs. C.E. Mur

Board member

Remedies Clause

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

decides 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 submission on paper is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague.

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

Write in your notice of objection at least:

- your name and address;
- the date of your objection;
- the reference referred to in this letter (case number); or enclose a copy of this decision;
- the reason(s) why you disagree with this decision;
- your signature.

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