Confidential/Registered

[CONFIDENTIAL]

Date

December 4, 2019

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 [CONFIDENTIAL],

The Dutch Data Protection Authority (AP) has decided to impose an administrative fine on [CONFIDENTIAL]. €725,000 to be imposed. The DPA is of the opinion that [CONFIDENTIAL] from 25 May 2018 to 16 April 2019 has the prohibition of Article 9, first paragraph, of the General Data Protection Regulation violated by processing biometric data of its employees.

The decision is explained in more detail below. Chapter 1 is an introduction and Chapter 2 describes it legal framework. In Chapter 3, the AP assesses whether biometric data is being processed, controller and the violation. In chapter 4 the (level of the) administrative penalty worked out and chapter 5 contains the operative part and the remedy clause.

December 4, 2019

Our reference

[CONFIDENTIAL]

1 Introduction

1.1 Legal entities involved and reason for the investigation

[CONFIDENTIAL] is a company registered at [CONFIDENTIAL]. [CONFIDENTIAL] is registered in the trade register of the Chamber of Commerce under number [CONFIDENTIAL]. [CONFIDENTIAL].

On July 5, 2018, the AP received a notification that employees at [CONFIDENTIAL] are required to have their fingerprint scanned. Supervisors of the AP concluded that from the report clocking in and out of employees using a fingerprint for time registration. Nasty

As a result of this signal, the AP has launched an official investigation into compliance by [CONFIDENTIAL] of Article 9 of the General Data Protection Regulation (GDPR), which under more on the use of processing biometric data, such as a fingerprint.

1.2 Process flow

On September 6 and October 12, 2018, the AP contacted the signaler by telephone to ask questions about his notification about (the obligation to) use and the locations of the fingerprint equipment at [CONFIDENTIAL]. In response to this, the AP on October 22, 2018 documents received from the signaller.

On November 6, 2018, the AP conducted an unannounced investigation at [CONFIDENTIAL]. The reports on this investigation and employee statements are as of February 11, 2019 sent to [CONFIDENTIAL]. [CONFIDENTIAL] has indicated no comments have on these documents.

On March 18, 2019, the AP again conducted an investigation at the office of [CONFIDENTIAL]. The reports on this investigation and the statements taken by employees were sent on 9 May 2019 to [CONFIDENTIAL].

The AP sent a draft report to [CONFIDENTIAL] on June 13, 2019. [CONFIDENTIAL]
gave its opinion on this on 3 July 2019. Taking this response into account, the AP has it
final report adopted. This report has been sent to [CONFIDENTIAL] by letter of 4 September 2019
sent.
In a letter dated September 16, 2019, the AP has sent [CONFIDENTIAL] an intention to enforce
sent. Also given the opportunity to do so by letter of 16 September 2019 by the AP
[CONFIDENTIAL] gave its opinion in writing on 21 October 2019 on this intention and the
final report on which it is based.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

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 on processing biometric data

Article 9(1) of the GDPR defines sensitive personal data as follows, insofar as relevant here:

“[...] personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data for the purpose of uniquely identifying a person, or data about health, or data related to someone's sexual behavior or sexual orientation […]”

Pursuant to Article 4, paragraph 14, of the GDPR, biometric data are personal data that the are the result of a specific technical processing with regard to the physical, physiological or behavioral characteristics of a natural person on the basis of which unambiguous identification of that natural person is possible or confirmed, such as facial images or fingerprint data.

Pursuant to Article 9, paragraph 1, of the GDPR, the processing of biometric data for the purpose of the unique identification of an individual is prohibited.

Exceptions to the prohibition on processing sensitive personal data are stated in Article 9, second paragraph, of the GDPR, insofar as relevant here:

“Paragraph 1 does not apply when one of the following conditions is met:

a) the data subject has given explicit consent to the processing of those personal data

for one or more specified purposes, except where Union or Member State law so provides

the prohibition referred to in paragraph 1 cannot be lifted by the data subject;

[…]

g) the processing is necessary for reasons of important public interest, based on Union law

or Member State law, ensuring proportionality with the aim pursued, the essential

content of the right to the protection of personal data is respected and appropriate and specific

measures are taken to protect the fundamental rights and interests of the

data subject;

[...]"

Pursuant to Article 4, paragraph 11, of the GDPR, consent is defined as any free, specific,

informed and unambiguous expression of will by the data subject by means of a statement or

an unambiguous active act accepts a processing of personal data concerning him.

Pursuant to Article 7(1) of the GDPR, the controller must be able to demonstrate that the

data subject has given permission for the processing of his personal data as the processing

based on consent. Pursuant to Article 7, paragraph 3, of the GDPR, the data subject has the right

withdraw consent at any time. Before the data subject gives his consent, he will be informed thereof

notified.

In accordance with Article 29 of the General Data Protection Regulation (UAVG) Implementation Act, attention has been paid

to Article 9(2)(g) of the Regulation, the ban on using biometric data with the

in order to process the unique identification of a person not applicable, if the processing

is necessary for authentication or security purposes.

2.3 Administrative fine

Pursuant to Article 58, paragraph 2, opening words and under i, in conjunction with Article 83, paragraph 5, opening words and

under

b, of the AVG and Article 14, third paragraph, of the UAVG, the AP is authorized with regard to infringements of the

AVG to impose an administrative fine.

2.3.1 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 4, 5 and 6
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.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

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.

2.3.2 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. Assessment

3.1 Processing of biometric personal data

3.1.1 Facts

At [CONFIDENTIAL], five scan stations are present and active, three of which have a finger scanner. One of
those three are used for testing and fingerprinting, the other two for

clocking in and out [CONFIDENTIAL]. All of these scan stations exchange data with one software program, with which, in addition to checking for presence and absence, people can gain insight into working hours, absenteeism and overtime.1

[CONFIDENTIAL] has stated that two fingers of her employees are fingerprints created and recorded. The scan station calculates a template of the fingerprint and stores it in the software program. This means that using a photographic scan unique dots identified in the lines of the printout. The dots together form the basis for one mathematical calculation to calculate the quality of the fingerprint template.2

[CONFIDENTIAL] has employee fingerprints recorded as soon as they are employed, so that one can clock in.3 Statements from the employees of [CONFIDENTIAL] show that they are summoned to come by for the fingerprinting.4

On March 18, 2019, the AP established that during the investigation at [CONFIDENTIAL]. [CONFIDENTIAL] owns a digital folder containing all fingerprint templates of fingerprints

1 Report of technical investigation during on-site investigation (dated 6 November 2018) of 12 November 2018, screenshot of website supplier of January 29, 2019 and technical investigation report including appendices A to H (appendix G (digital content folder bio_templates) and appendix H (digital photo files) dated March 19, 2019.

2 Report of technical investigation during on-site investigation (dated 6 November 2018) dated 12 November 2018.

3 Conversation report with director of [CONFIDENTIAL] of 9 November 2018.

4 First three conversation reports with employees of [CONFIDENTIAL] of 7 November 2018 and conversation reports with employees of [CONFIDENTIAL] dated 19 March 2019.

of employees ever scanned at [CONFIDENTIAL]. These templates are saved as text files.5

The AP has determined that from the contents of this folder it can be deduced what the period is within fingerprints of employees are recorded. The fingerprint templates are stored in this folder as [CONFIDENTIAL] files. The [CONFIDENTIAL] files belong to employees who are in service of [CONFIDENTIAL]. The [CONFIDENTIAL] files belong to former employees of [CONFIDENTIAL]. When the fingerprint templates belong to the affected employee created can be deduced from the date in the separate text files of the templates. For [CONFIDENTIAL] files, the storage date also corresponds to the date of recording of the fingerprint, which is contained in the text file itself.

The first fingerprint templates were saved on January 23, 2017. From then on, are regular templates saved. The latest employee fingerprint templates are dated November 8, 2018.

From the storage data of the [CONFIDENTIAL] files it follows that of 39 employees after May 25, 2018 fingerprint templates are created. This follows from the storage data of the [CONFIDENTIAL] files May 25, 2018 of 31 employees fingerprint templates were created. From the content of the [CONFIDENTIAL] files deduce that of 17 employees after May 25, 2018 fingerprint templates are created. In total, after 25 May 2018, there are therefore (39+31+17=) 87 employees fingerprints captured and stored. The AP has determined that on March 18, 2019, a total of 1348 fingerprint templates (as [CONFIDENTIAL] files) are stored in this folder. Because per employee four fingerprint templates are stored, so these are the fingerprints of (1348:4=) 337 (former) employees of [CONFIDENTIAL].6

[CONFIDENTIAL] has stated that of employees who have had their fingerprints recorded and that were in service on March 18, 2019, the fingerprint templates were actually active on March 18, 2019 in the software program and the scan stations.7 The AP determined this in part on the basis of a personnel card of an employee who was employed at the time. On the relevant personnel card fingerprint templates are active. The personnel card also shows that there is a quality indication of the

fingerprints and that the fingerprints of this employee were recorded on November 8, 2018.8

[CONFIDENTIAL] has further stated that of employees who are out of service and on March 18, 2019

processed in the software program in such a way that no more fingerprint templates are present in it

software program and the scan stations. When an employee leaves employment, his/her data becomes

according to [CONFIDENTIAL] kept, but blocked in the software program.9 This has

5 Technical research report including appendices A to H (appendix G (digital content folder bio_templates) of 19 March 2019.

6 Technical research report including appendices A to H (appendix G (digital content folder bio_templates) of 19 March 2019.

7 Technical investigation report including appendices A to H of 19 March 2019.

8 Technical investigation report including appendices A to H, appendix E (printout of file “people employed with finger

scan.pptx”) p.

9, dated March 19, 2019.

9 Conversation report with [CONFIDENTIAL] at [CONFIDENTIAL] of 9 November 2018.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

[CONFIDENTIAL] partly illustrated to the AP on the basis of a number of personnel cards from

persons who left employment on March 18, 2019.10

On March 18, 2019, the AP took 160 screenshots of employee cards from employees

whose fingerprint templates were active in both the software program and the scan stations.11 Also

[CONFIDENTIAL] came from the number of [CONFIDENTIAL] files in that folder

concluded that on March 18, 2019, fingerprint templates of 160 employees were active in the

software program and the scan stations.12

Based on the above, the AP concludes that after the fingerprint has been recorded, the templates

of those fingerprints are stored as a text file in a digital folder. These templates from

fingerprints that have been recorded since the beginning of 2017 are therefore still stored there. This also applies for employee fingerprint templates that are out of service, although they will then be blocked and are no longer active in the software program and scan stations.

Production employees of [CONFIDENTIAL] can only clock in and out with their use fingerprint and the drop (an identification tag) separately and side by side and do so also regularly. Based on the template in the software program, their identity is displayed on the device attached. It cannot be determined from the time registration in the software program whether a fingerprint or a drop is clocked in or out.13

[CONFIDENTIAL] has stated that on November 6, 2018, the finger scanning equipment has only been used since a small years of continuous use.14 Several employees of [CONFIDENTIAL] have stated that the scan stations will be used from 2017.15

During the visit on March 18, 2019, [CONFIDENTIAL] indicated that after the AP's visit on November 6, 2018 [CONFIDENTIAL] has stopped scanning the fingerprints of (new) employees, because people no longer know whether or not it is allowed.16 On 18 March 2019, the AP also found that [CONFIDENTIAL] no new fingerprints since November 8, 2018 has recorded.

[CONFIDENTIAL] received instructions from the supplier on April 16, 2019 on how to remove it of the software and the files contained therein. [CONFIDENTIAL] has stated that she is flat

10 Technical investigation report including appendices A to H of 19 March 2019, p. 2 and 3.

11 Technical investigation report including appendices A to H, appendix E (printout of file “people employed with finger scan.pptx”), of March 19, 2019.

12 Technical research report including appendices A to H (appendix G (digital content folder bio_templates) of 19 March 2019.

13 First three conversation reports with employees of [CONFIDENTIAL] of 7 November 2018, conversation report with director of [CONFIDENTIAL] of November 9, 2018, conversation report with [CONFIDENTIAL] at [CONFIDENTIAL] of November 9 2018 and technical investigation report on site investigation (dated November 6, 2018) dated November 12, 2018.

14 Conversation report with director of [CONFIDENTIAL] of 9 November 2018.

15 Second and third interview report with employees of [CONFIDENTIAL] of 7 November 2018 and interview report with [CONFIDENTIAL] to [CONFIDENTIAL] dated 9 November 2018.

16 Report of official acts of the on-site investigation at [CONFIDENTIAL] (dated 6 November 2018) dated 12 November 2018.

has subsequently removed and has the biometric data of its (former) employees log files as proof of deletion.17 It can be seen from the log files that the biometric data has actually been deleted but the exact date on which this happened can be cannot be deduced from this.18 In view of this, the AP assumes that the violation will in any event be up to and has continued through April 16, 2019.

3.1.2 Assessment

According to Article 4, paragraph 1, of the GDPR, personal data includes all information about a identified or identifiable natural person (“the data subject”). If becomes identifiable considered a natural person who can be identified directly or indirectly, for example by one or more elements characteristic of the physical or physiological identity of that natural person.

Pursuant to Article 4, fourteenth paragraph, of the GDPR, biometric data includes personal data which are, among other things, the result of a specific technical operation related to the physical characteristics of a natural person, on the basis of which unambiguous identification of that natural person person is possible or confirmed. Fingerprint data is explicitly mentioned as example of biometric data.

Article 4, second paragraph, of the GDPR defines the concept of processing as an operation of

personal data, such as the collection, recording, storage, retrieval, consultation or use thereof.

The AP has established that [CONFIDENTIAL] has fingerprints of 337 (former) employees
stored from January 23, 2017 to at least April 16, 2019. As the facts show, these
fingerprints are stored as templates and they remain stored there even when employees are already out of service
are. The fingerprint templates of employees who are (still) employed are linked to a
software program so that they can clock in and out with their fingerprint. Employees of
[CONFIDENTIAL] since 2017 regularly use their fingerprint on the fingerprint scanner to
and clocking out, using the template in the software program to identify their identity
confirmed. By simply capturing the fingerprints of employees, further measures can therefore be taken
processing of the fingerprint, such as using the fingerprint to check in and out
bells.

The AP comes to the conclusion that the data stored by [CONFIDENTIAL] is natural
persons, namely its employees, can be identified. The data is the result of
a specific technical operation related to the physical characteristics of a natural person
(the fingerprint), on the basis of which unambiguous identification of that natural person is possible
is confirmed to employees via the fingerprint device. Therefore, it is biometric
data within the meaning of Article 4, part fourteen, of the GDPR. As far as [CONFIDENTIAL] argues

17 Written response from [CONFIDENTIAL] dated 13 November 2019, question 2 and annex 2.

18 Written response from [CONFIDENTIAL] dated 13 November 2019, question 1 and log file.

that the code, which is created on the basis of the fingerprint, cannot be traced back to an employee
the AP does not accept this conclusion of [CONFIDENTIAL].19

[CONFIDENTIAL] has digitally stored the fingerprint data and also processes it
by means of the finger scanning equipment when making the fingerprint and when employees use their finger
scan to clock in and out. The AP comes to the conclusion that [CONFIDENTIAL] because of this
has processed biometric data (partially) automatically within the meaning of Article 4, part
two, from the GDPR.

3.1.3 Conclusion

[CONFIDENTIAL] had stored biometric data of 250 employees on May 25, 2018, which
gradually increased to 337 employees. [CONFIDENTIAL] has until at least April 16
2019 processed the biometric data. In view of the foregoing, the AP concludes that
[CONFIDENTIAL] employee biometric data from May 25, 2018 through April 16, 2019
has processed within the meaning of Article 4, part fourteen, of the GDPR.

3.2 Controller

The AP is of the opinion that [CONFIDENTIAL] the purposes and means for the processing of the
determined biometric data. [CONFIDENTIAL] has made the decision to remove the
deploying (and financing) fingerprint scanning equipment as a means of obtaining biometric data
process its employees.20
[CONFIDENTIAL] has also determined the purpose of the processing, namely the reduction of
abuse when clocking in and out for time registration. According to [CONFIDENTIAL] and is in it
In the past, it regularly happened that one employee clocked in for two employees while only one
person was present. There were also practical purposes, according to [CONFIDENTIAL]. There are none like that
costs for the purchase, loss or damage of drops.21 Employees also give the reason that
the system offers a conclusive attendance registration, that the system with finger scanners the
outdated system with drop scanners and that it can be part in the future
of the security of the computer network (hacking attempts, industrial espionage).22

19 See also Rb. Amsterdam 12 August 2019, ECLI:NL:RBAMS:2019:6005, in which it was held that a fingerprint converted
was to a code is a (biometric) personal data within the meaning of the AVG.

20 Report of conversation with director of [CONFIDENTIAL] of 9 November 2018, report of conversation with

[CONFIDENTIAL] at

[CONFIDENTIAL] of 9 November 2018, overview list and copied documents during the on-site investigation (dated 6

November

2018) of November 12, 2018 document no. 17 and no. 18, and report technical investigation during on-site investigation (dated

November 6

2018) of November 12, 2018.

21 Report of conversation with director of [CONFIDENTIAL] of 9 November 2018 and report of official acts of investigation for

place (d.d. March 18, 2019) at [CONFIDENTIAL] dated March 19, 2019.

22 Report of conversation with [CONFIDENTIAL] at [CONFIDENTIAL] of 9 November 2018 and report of technical

investigation at

on-site investigation (dated November 6, 2018) of November 12, 2018.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

Based on the above, the AP designates [CONFIDENTIAL] as the controller

as referred to in Article 4, part 7, of the GDPR.

3.3 Prohibition on processing biometric data

3.3.1 Introduction

In recent years, the importance of biometric data for the identification of persons has become strong

increased. New compared to previous legislation is the fact that the GDPR biometric data

are processed for the purpose of uniquely identifying a person, also designated as a special one

category of personal data.23

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.24
In the following, the AP assesses whether [CONFIDENTIAL] can successfully rely on this case
relevant exceptions as referred to in Article 9, second paragraph, under a and g, of the GDPR. In this respect
processing based on “explicit consent” or “necessary for
authentication or security purposes”.

3.3.2 Facts

The employment contracts used by [CONFIDENTIAL] do not contain any information about the
use of fingerprints.25 The personnel handbooks applicable at the time, dated July 2017,
report the following: “[CONFIDENTIAL]”.26
On November 6, 2018, the AP received a copy of a draft version of amendments to the
production personnel manual. The above paragraph on attendance registration was unchanged
remained.27 In an updated version of the handbooks, which are dated January 2019, the sentence
“[CONFIDENTIAL]” omitted.28
Several employees of [CONFIDENTIAL] have stated that recording the
fingerprints came as a surprise, had not been announced and that they had no information about this
received.29 The AP has inquired about documentation of policies or procedures for or evidence

23 See Parliamentary Papers II 2017/18, 34851, 3, p. 40 and 108 (MvT).

24 See recital 51 of the GDPR.

25 Overview list and copied documents during the on-site investigation (dated 6 November 2018) of 12 November 2018, no. 3,
4, 5
and 6.

26 Overview list and copied documents during the on-site investigation (dated 6 November 2018) of 12 November 2018, no. 7
and 8.

27 Overview list and copied documents during the on-site investigation (dated 6 November 2018) of 12 November 2018, no. 9.

28 Overview list and copied documents during on-site investigation (dated March 18, 2019) dated March 19, 2019.

29 First three conversation reports with employees of [CONFIDENTIAL] of 7 November 2018 and first conversation report with employee of [CONFIDENTIAL] dated 19 March 2019.

of granting permission to take fingerprints and refusing to do so. Of such documentation was not available.

The director of [CONFIDENTIAL] has stated that he has no idea whether the processing of the fingerprints permission is requested from the employees, but that it is a free choice.30

The [CONFIDENTIAL] has stated that employees do not consent to the use of their fingerprint, but that scanning the fingerprint is not mandatory. They do sign up reception of the drop.31

The [CONFIDENTIAL] further indicates that there is a possibility to collect the fingerprints to refuse. To this end, the employee concerned must enter into a discussion with the director. In the in practice this is almost non-existent. In the few cases where this has occurred, the employee has after the his or her fingerprint was still given in a meeting with the director.32

A [CONFIDENTIAL] has stated that with regard to consent to the employment contract and the employee handbook, on the basis of which it considers it to be known by employees that [CONFIDENTIAL] wants to work with fingerprints in the future.33

Regarding the answer to the question of whether permission is requested to take fingerprints, There is a mixed picture among employees on the shop floor. On the one hand, employees indicate that fingerprint scanning was mandatory. On the other hand, there are two employees who declare that they have given oral consent.34

For testing whether the processing is necessary for authentication or security purposes, the

following facts are important.

The business activities of [CONFIDENTIAL].35 [CONFIDENTIAL].36

As mentioned in section 3.1.1. [CONFIDENTIAL] uses a time registration software

and – on that basis – the administration of salary, leave and illness. The presence of employees

in the past was only recorded by clocking in and out with drops at

scan stations.37

30 Interview report with director of [CONFIDENTIAL] of 9 November 2018.

31 Conversation report with [CONFIDENTIAL] at [CONFIDENTIAL] of 9 November 2018.

32 Report of technical investigation during on-site investigation (dated 6 November 2018) of 12 November 2018.

33 Conversation report with [CONFIDENTIAL] at [CONFIDENTIAL] of 9 November 2018.

34 First three conversation reports with employees of [CONFIDENTIAL] of 7 November 2018 and conversation reports with

employees of [CONFIDENTIAL] dated 19 March 2019.

35 Chamber of Commerce extract [CONFIDENTIAL] of 15 October 2018.

36 Technical investigation report on site investigation (dated 6 November 2018) dated 12 November 2018.

37 Interview report with director of [CONFIDENTIAL] of 9 November 2018 and interview report with [CONFIDENTIAL] at

[CONFIDENTIAL] dated 9 November 2018.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

The director of [CONFIDENTIAL] has decided to expand the time registration system with the

finger scanning equipment. He made the decision independently in his capacity as general

director of [CONFIDENTIAL].38 As stated in section 3.2, the reason for this was the

reducing abuse when clocking in and out for time registration. There were according

[CONFIDENTIAL] also practical benefits. There are no costs for purchase, loss or drop damage. Employees also cite the reason that the system is a watertight one attendance registration, that the system with finger scanners replaces the outdated system with drop-scanners and that in the future it can be part of the security of the computer network (hacking attempts, industrial espionage). Finally, by using finger identification only persons who are trained in the use of advanced equipment enter.

3.3.3 Assessment

3.3.3.1 Explicit Consent

Under Article 4(11) of the GDPR, consent is free, specific, informed and unambiguous expression of will with which the data subject by means of a statement or a unequivocally active act accepts a processing of personal data concerning him.

In order for informed consent to be given, the data subject must be informed, among other things be informed about the identity of the controller, the purpose of the processing, which (type) data are processed and the existence of the right to withdraw consent.39

In addition, a data subject must be able to freely give consent. In the Guidelines on consent in accordance with the GDPR is noted about this:

“Disproportion also occurs in the context of the employment relationship. Given the dependency that results from the relationship between employer and employee, it is unlikely that the data subject has given his/her consent data processing could withhold without fear or real threat of adverse consequences as a result refusal. It is unlikely that the employee could freely respond to a request for consent from his/her employer for, for example, activating surveillance systems such as camera surveillance in the workplace, or the filling out assessment forms, without feeling pressured to give permission. That's why WP29 believes that it is problematic for employees to process personal data of current or future employees on based on consent, as it is unlikely to be freely granted. For the majority of such data processing at work, the legal basis cannot and must not be the consent of the employees (Article 6(1) under a) due to the nature of the relationship between employer and employee. However, this does not mean that employers

never

may rely on consent as a legal basis for processing. There may be situations where the employer

can demonstrate that consent is actually freely given. Given the mismatch between an employer and

his staff, employees can only give their consent freely in exceptional circumstances, and when

38 Report of conversation with director of [CONFIDENTIAL] of 9 November 2018, report of conversation with

[CONFIDENTIAL] at

[CONFIDENTIAL] dated 9 November 2018 and technical investigation report on site investigation (dated 6 November 2018) of

November 12, 2018.

39 See recital 42 of the GDPR, the Guidance on consent under Regulation 2016/679 dated 28 November

2017 p. 15 and Article 7, third paragraph, of the GDPR.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

it has no negative consequences if they give their consent or not. […] Mismatches are not limited to

government agencies and employees, they can also arise in other situations. Like WP29 in different

Opinions has emphasized, "consent" can only be legally valid if the data subject has a real choice and there

there is no question of deception, intimidation or coercion and the person concerned is not at risk of significant negative

consequences

(e.g. at significant additional cost) if he or she does not agree. Consent is not free in cases where

there is any element of coercion, pressure or inability to exercise free will".40

Pursuant to Article 7(1) of the GDPR, the controller must also be able to

demonstrate that the data subject has given consent to the processing of his personal data.

The conditions of Article 7 of the GDPR also apply to the concept of consent in Article 9 of the GDPR

GDPR.41 To meet the condition of Article 9(2)(a) of the GDPR for exemption

the prohibition of processing biometric data of Article 9, first paragraph, of the GDPR applies –
in addition to the conditions that Article 7 GDPR sets for consent - that the data subject expressly
must give permission.
According to the Guidance on Consent under the GDPR, explicit refers
consent to the way consent is expressed by the data subject. Hereby
according to the Guidelines, written permission, signature (possibly
with electronic signature), the sending of an e-mail or consent by the data subject
two-step verification. In theory, the use of verbal statement may also be sufficient to make valid
to obtain explicit consent, however, it may be difficult for the controller to do so
proof that all conditions for validity have been met when the statement is included
express consent.42
Based on the following facts, the AP concludes that [CONFIDENTIAL] does not have
demonstrated that its employees have given explicit consent to the processing of
their biometric data. The free, specific, informed and unambiguous expression of the will of the
employees of [CONFIDENTIAL] has not been established.
[CONFIDENTIAL], as a controller, has not demonstrated that its employees
have given (explicit) permission at all for the processing of the biometric
data, which is mandatory under Article 7(1) of the GDPR. It can be seen from paragraph 3.3.2
after all, [CONFIDENTIAL] has no documentation of policies or procedures for or evidence of it
granting permission to record fingerprints and refusing to do so. Thereby
several employees stated that the scanning of the fingerprints was mandatory and that
no permission is requested for this, not even in the context of signing the
employment contract or receipt of the employee handbook. Two employees have stated that
40 Guidance on consent under Regulation 2016/679 dated 28 November 2017, pp. 7-8. Last revised
and adopted by the Article 29 Data Protection Working Party on 10 April 2018.
41 Guidance on consent under Regulation 2016/679 dated 28 November 2017, p. 23.

42 Guidance on consent under Regulation 2016/679 dated 28 November 2017, pp. 20-22.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

they have given oral permission for their fingerprint to be recorded.

However, [CONFIDENTIAL] also has the existence of any oral statements about

unable to prove consent. [CONFIDENTIAL] has therefore not been able to demonstrate that her

employees have explicit consent within the meaning of Article 9, paragraph 2, under a, of the GDPR

given for the processing of their biometric data.

Needless to say, the AP notes that [CONFIDENTIAL] was also unable to demonstrate that her

employees were sufficiently informed about the processing of the biometric data and that they

freedom have given their consent. As mentioned in section 3.3.2, there was in the

employment contract does not include information about the use of fingerprints. Employees

have only been informed through the July 2017 employee handbook that [CONFIDENTIAL] the intention

to start clocking in completely with the fingerprint. In the most recent employee handbook of

January 2019 there is nothing left about the intention to switch completely to time registration with the

fingerprint. Several employees of [CONFIDENTIAL] have also stated that the

recording of the fingerprints had not been announced and that they have no information about this

received.

In addition, [CONFIDENTIAL] has not demonstrated that any consents given are freely passed on

its employees are given. In addition, employees of [CONFIDENTIAL] have stated that the

fingerprint scanning was mandatory. And have the [CONFIDENTIAL] and an employee

stated that in case of refusal to have the fingerprint scanned, a meeting with the director/board

followed, after which (almost) everyone has their fingerprint scanned in practice.

It follows from the above that – despite the fact that [CONFIDENTIAL] believes that there is a freedom of choice
employees to whether or not to clock in and out using their fingerprint – different ones
employees have experienced it as an obligation to have their fingerprints recorded. Between the
There is a hierarchical relationship between the employer and the employee. Given the dependency that
results from the relationship between employer and employee, it is unlikely to be the employee
or freely grant its consent. Moreover, [CONFIDENTIAL] has not shown that in
in this case freely given permission.

[CONFIDENTIAL] must, pursuant to Article 7, paragraph 1, of the GDPR demonstrate that a data subject
has given permission for the processing of his personal data. The conditions of Article 7
of the GDPR also apply to the concept of consent in Article 9 of the GDPR. On the basis of it
above, the AP is of the opinion that [CONFIDENTIAL] has not been able to demonstrate that her
employees have explicit consent within the meaning of Article 9, paragraph 2, under a, of the GDPR
given for the processing of their biometric data.

Opinion [CONFIDENTIAL] and response AP

[CONFIDENTIAL] believes that the employees have given permission for the use
of their fingerprints and that no one has ever objected to it. The system with the
drop was also perceived as inconvenient by many employees. [CONFIDENTIAL] is always very open

about the use of the fingerprint system and had only good intentions.
It has also never been an obligation to clock in and out with the fingerprint; this was always possible
still with the drop. [CONFIDENTIAL] is therefore of the opinion that the employees are free to use their
could have given permission. It is also by no means correct that employees who do not have their fingerprint

wanted to have it taken, had a meeting with the management. No one is according to [CONFIDENTIAL]
forced to use the finger scans and the ability to use the drip system,
has always existed. In fact, of the 4 drop clocks present, only 2 are additional
equipped with the finger scan option.
[CONFIDENTIAL] indicates, after the first visit of the AP on November 6, 2018, immediate measures
taken and stopped clocking in and out using fingerprints. After that
date, fingerprints are no longer recorded either. After the AP's second visit on March 18, 2019
[CONFIDENTIAL] has contacted the supplier of the fingerprint equipment and has obtained the
conducted fingerprint scans and leave the program with regard to registration with fingerprints
to delete. [CONFIDENTIAL] wanted to ensure that all biometric data as soon as possible
would be destroyed so that [CONFIDENTIAL] would not be at any further risk. The supplier has
indicated to [CONFIDENTIAL] that the use of the finger scan is allowed in this, because this
is not mandatory and 2 scan options are offered by [CONFIDENTIAL]: the finger scan
and the drop.
The AP interprets the view in such a way that [CONFIDENTIAL] is of the opinion that the employees are free to use their
have been able to give permission for the processing of the fingerprints. The AP follows the view
of [CONFIDENTIAL]. Given the dependence that results from the relationship between employer
and employee, it is unlikely that the employee can freely give his or her consent.
If in this exceptional case there was free consent, then [CONFIDENTIAL] had this
must demonstrate. [CONFIDENTIAL] has provided no evidence that its employees consent
have given for the processing of the fingerprints, let alone consent freely and
informed is given. In addition, several employees, despite the freedom of choice for
employees whether or not to clock in and out using their fingerprint, it as an obligation
experienced to have their fingerprint recorded.
3.3.3.2 Necessary for authentication or security purposes
Article 9(2)(g) of the GDPR leaves room for an exception in national law

prohibition to process biometric data for reasons of important public interest. In
The Netherlands has implemented this in Article 29 of the UAVG, by processing biometric
allow data if the processing is necessary for authentication or security purposes.
Furthermore, the Explanatory Memorandum to Article 29 of the UAVG states that it is undesirable not to
national exemption for the processing of biometric data. Furthermore, here it says:
“It must be weighed up whether identification with biometric data is necessary for this
authentication or security purposes. The employer will then have to consider whether the buildings and information systems
must be secured in such a way that this must take place with biometrics. This will be the case if access is restricted

should be to certain persons who are authorized to do so, such as at a nuclear power plant. The processing of
biometric data should also be proportional. When it comes to accessing a repair shop garage,
will the need for security not be such that employees can only access with biometrics and
to this end, this data is recorded in order to exercise access control. On the other hand, sometimes biometrics can
are an important form of security for information systems, for example, which themselves contain a lot of personal data
contain unauthorized access, including by employees, must be prevented. To make this assessment possible
in circumstances where consent cannot be freely given is a provision in the bill
which allows for an exception to the ban on the processing of biometric data for the purpose of
the identification of the data subject, if this is necessary for authentication or security purposes”.43
As the Explanatory Memorandum states, a consideration must be made whether identification by means
of biometrics is necessary and proportionate for authentication or security purposes.
[CONFIDENTIAL] should have considered whether the buildings and information systems of
[CONFIDENTIAL] must be secured in such a way that it must be done with biometric data

find. There is a strict test for this. For example, biometrics may be used at a nuclear power station for access control. Security is very important there and only certain people are allowed have access. [CONFIDENTIAL] should also have considered whether to process fingerprints of employees at [CONFIDENTIAL] is proportionate. The use of biometric personal data when accessing, for example, the garage of a repair company, this key cannot to endure. After all, the need for security is not so great that people continue to use it biometrics should be allowed access. In addition, security can also be reduced in other ways far-reaching ways.

As stated in paragraph 3.3.2, [CONFIDENTIAL]'s business activities include, among other things [CONFIDENTIAL]. [CONFIDENTIAL] according to [CONFIDENTIAL] simple work is done, such as [CONFIDENTIAL]. [CONFIDENTIAL] is also used according to [CONFIDENTIAL]. advanced equipment to make it.

[CONFIDENTIAL] uses the relevant software program for time registration and - based of which – the administration of salary, leave and illness. The presence of workers was in it past recorded only by clocking in and out with drops at scan stations. The director of [CONFIDENTIAL] has independently decided to expand the time registration system with the fingerprint equipment. As stated in section 3.2, the reason for this was to reduce abuse when clocking in and out for time registration. There were also according to [CONFIDENTIAL]. practical benefits. There are no costs for the purchase, loss or damage of drops.

Employees also give the reason that the system offers a comprehensive attendance registration, that the system with finger scanners should replace the outdated system with drop scanners and that the may be part of the security of the computer network in the future (hacking attempts, corporate espionage). Finally, by using finger identification, only persons can do it who are trained in the use of advanced equipment.

43 Parliamentary Papers II 2017/18, 34851, 3, p. 94-95 (MvT).

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

The AP is of the opinion that the processing of biometric data in the context of (preventing abuse in) time registration, attendance control and authorized use of equipment in [CONFIDENTIAL] is not necessary and proportionate. The previously described activities [CONFIDENTIAL], including [CONFIDENTIAL], approach the work earlier within a garage of a repair company, where, according to the Explanatory Memorandum to Article 29 of the UAVG is not necessary and proportionate to process biometric data. Admittedly [CONFIDENTIAL] has an interest in working with finger scanning equipment for (countering abuse in) time registration, but in view of this purpose and the business activities of [CONFIDENTIAL] does that interest not justify an exception to the ban on the processing of biometric data. Just as with a garage, also with [CONFIDENTIAL] the need for security is not such that employees must be able to gain access with biometrics and this data must be recorded for this purpose to exercise access control. In addition, other ways, which infringe less on the privacy of employees, also achieve this.

[CONFIDENTIAL] has indicated that he agrees with the draft report of the AP's findings with the AP stating that the ground for exception is 'necessary for security or authentication' [CONFIDENTIAL] may not apply. According to [CONFIDENTIAL] this is the main reason to [CONFIDENTIAL] stop using biometric data for access control.

[CONFIDENTIAL] has not given any opinion on this on the final report of the investigation ground for exception.

Based on the above, the AP is of the opinion that there is no need for [CONFIDENTIAL]. to prohibit the processing of biometric data in the context of authentication or justifiable security purposes. [CONFIDENTIAL] may be concerned with the processing of

fingerprints therefore do not invoke the possibility of derogation in Article 9, paragraph 2, under

g, of the GDPR in conjunction with Article 29 of the UAVG.

3.3.4 Conclusion

Pursuant to Article 9, paragraph 1, of the GDPR, it is in principle prohibited to use biometric data

process. The AP comes to the conclusion that the processing of biometric data is subject to

responsibility of [CONFIDENTIAL] does not meet the conditions for an exception to it

prohibition of Article 9 of the GDPR specifically does not meet the conditions referred to in Article 9,

second paragraph, under a, of the GDPR or Article 9, second paragraph, under g, of the GDPR, read in conjunction with

Article 29 of the UAVG. With this [CONFIDENTIAL] the prohibition of Article 9, first paragraph, of the

GDPR violation.

3.4 Final conclusion

The AP comes to the conclusion that [CONFIDENTIAL] as controller of May 25, 2018

up to and including 16 April 2019, has violated the prohibition of Article 9, paragraph 1, of the GDPR by using biometric

process data of its employees.

4. Fine

4.1 Introduction

[CONFIDENTIAL] has from 25 May 2018 to 16 April 2019 the prohibition of Article 9, first paragraph, of

violated the GDPR by processing biometric data of its employees.

For the established violation, the AP uses its authority to [CONFIDENTIAL]

to impose a fine pursuant to Article 58, second paragraph, opening words and under i and Article 83, fifth paragraph, of the

AVG, read in conjunction with Article 14, third paragraph, of the UAVG. The AP uses the

Fining Policy Rules 2019.44

After this, the AP will first briefly explain the fine system, followed by the reasons for the fine

fine in this case.

4.2 Fining Policy Rules of the Dutch Data Protection Authority 2019 (Fining Policy Rules 2019)

Pursuant to Article 58, second paragraph, opening words and under i and Article 83, fifth paragraph, of the GDPR, read in

connection with Article 14, third paragraph, of the UAVG, the AP is authorized to inform [CONFIDENTIAL] in case of

to impose an administrative fine of up to € 20,000,000 for a violation of Article 9, paragraph 1, of the GDPR, or

up to 4% of the total worldwide annual turnover in the previous financial year, whichever is higher.

The AP has established Fining Policy Rules 2019 regarding the implementation of the aforementioned power to

imposing an administrative fine, including determining the amount thereof.45

Pursuant to Article 2, under 2.2, of the Fining Policy Rules 2019, the provisions regarding violation

of which the AP can impose an administrative fine not exceeding € 20,000,000 or, for

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

is higher, classified in Annex 2 as Category I, Category II, Category III or Category IV. The penalty categories

are ranked according to the seriousness of the offence, with category I containing the least serious offences

and category III or IV the most serious offences.

In Annex 2, Article 9 of the GDPR is classified in category IV.

Pursuant to Article 2, under 2.3, the AP sets the basic fine for violations for which a legal

maximum fine of € 20,000,000 or, for a company, up to 4% of the total worldwide

annual turnover in the previous financial year, if this figure is higher, [...] fixed within the next

fine bandwidth:

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

44 Stct. 2019, 14586, March 14, 2019.

45 Ditto.

December 4, 2019

Our reference

[CONFIDENTIAL]

Pursuant to Article 6, the AP determines the amount of the fine by increasing the amount of the basic fine (to at most the maximum of the bandwidth of the fine category linked to a violation) or down (to at least the minimum of that bandwidth). The base fine is increased or decreased depending on the extent to which the factors referred to in Article 7 are used give rise.

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 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

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, the penalty bandwidth of the next higher or the next

apply lower category. In addition, the AP assesses when imposing an administrative fine

pursuant to Section 5:46(2) of the Awb, to what extent this can be attributed to the offender.

4.3 Fine amount

4.3.1. 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 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. Serving Stakeholders therefore have a high degree of control over their biometric 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 GDPR are possible. With fingerprinting and the subsequent retention of biometric data [CONFIDENTIAL]x has the high in this case level of protection offered by Article 9, first paragraph, of the GDPR.

[CONFIDENTIAL] has biometric data from its employees processed. This violation has therefore taken place in a structural manner and for one continued for a longer period. During this period, [CONFIDENTIAL] also has the biometric data of former employees kept, when there was no need for this. During this During this period, the data subjects have therefore had no control over their biometric data.

On the one hand, [CONFIDENTIAL] encrypted the biometric data and stated that only a limited number of people had access to the data. On the other hand, the fact that [CONFIDENTIAL] on May 25, 2018 had stored biometric data of 250 employees, which number is gradual increased to 337 employees, there was a systematic and structural breach.

In view of the fact that the violation lasted more than ten months, involving 337 people affected, a serious situation has arisen. [CONFIDENTIAL] not only has the biometric data of current employees but also of former employees without need stored for a longer period of time. In addition, the employees were insufficiently informed about the processing and it is not established that they (freely) gave permission, which in the opinion of the AP there is a serious violation in which the special data of those involved are incorrect conditions have been processed.

As a result, a large group of [CONFIDENTIAL] employees did not know for which purpose purposes the fingerprints were used and that they could give their consent at all times to withdraw. As a result, those involved had no control over what happened to them for a longer period of time

biometric data happened at [CONFIDENTIAL]. And it is precisely this control that the GDPR addresses
wants to offer data subjects, so that data subjects are able to protect their personal data and this
to be free to surrender. The AP is therefore of the opinion that there has been a serious violation,
but sees no reason in this case to increase or decrease the fine amount.

4.3.2 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.

Pursuant to Article 9, paragraph 1, of the GDPR, it is in principle prohibited to use biometric data
process. The GDPR applies from May 25, 2018 and dates from April 27, 2016.
Controllers have had two years until 25 May 2018 to submit their
bring processing activities into line with the AP.

[CONFIDENTIAL] In October 2016, well after the publication of the GDPR, the finger scanning equipment
purchased from a supplier. According to [CONFIDENTIAL], this supplier has no
pointed out a possible conflict with (future) privacy regulations and she trusted that
inform this professional party [CONFIDENTIAL] of changes. The AP is from
judge that this circumstance does not exculpate [CONFIDENTIAL]. That is the starting point
[CONFIDENTIAL] has its own responsibility to act from the entry into force of the
AVG to comply with the rules set therein. [CONFIDENTIAL] has failed to self-process
of the biometric data against the GDPR or to obtain legal advice on this. Instead
of which [CONFIDENTIAL] assumed that a third party, with a commercial interest in the
sale of the equipment, assumed this responsibility. From a professional party like

[CONFIDENTIAL] may be expected, partly in view of the special nature of the personal data that it is thoroughly aware of the standards that apply to it and that it complies with them. [CONFIDENTIAL] has violated the high level of protection for special personal data by its conduct. The AP considers this culpable.

4.3.3 Opinion [CONFIDENTIAL] and response AP

[CONFIDENTIAL] argues in its view that on the basis of the factors of Article 83, second paragraph, of the GDPR and the Guidelines for the application and determination of administrative fines of 3 October 2017, a fine is not appropriate and if a fine is nevertheless imposed imposed, it must be moderated by the AP. [CONFIDENTIAL] believes that if there is of a violation of the GDPR, it would not be reasonable/opportune to impose a fine. In this case, according to [CONFIDENTIAL], a reprimand is an appropriate measure, which is sufficiently effective, proportionate and dissuasive. The AP sets out the points from [CONFIDENTIAL]'s opinion below briefly, accompanied by a response from the AP.

With regard to the nature, seriousness and duration of the infringement, [CONFIDENTIAL] is first of all of the opinion that this infringement in the concrete circumstances of the case does not pose a significant risk to the rights of the data subjects and does not detract from the substance of the obligation concerned.

[CONFIDENTIAL] has used the fingerprints for the collection and processing from a professional company and a professional program, with the security of the data guaranteed and not used for other purposes. Those involved have said [CONFIDENTIAL] also suffered no damage and will not suffer any damage, now the affected data have since been destroyed. The number of people involved is also limited in this respect

[CONFIDENTIAL], regarding employees of [CONFIDENTIAL] in the period January 2017 to November 2018. Immediately after the AP's first visit, [CONFIDENTIAL] stopped collecting of fingerprints and after the second visit in March 2019, [CONFIDENTIAL] has ensured that all relevant data was destroyed. Incidentally, [CONFIDENTIAL] notes with regard to the is still pending, that the AP already on July 5, 2018 (just over a month after the GDPR came into force) received a notification about the finger scans. The AP's first investigation wasn't until Nov. 6 2018 and the second examination on March 18, 2019. If [CONFIDENTIAL] earlier, that is, immediately after the notification (when the GDPR had just entered into force), she had to take measures earlier.

The AP does not follow this view of [CONFIDENTIAL]. [CONFIDENTIAL] should have in this case fail to process the biometric data of its employees. By doing so, you have [CONFIDENTIAL] violated the substance of this obligation. Because the employees of [CONFIDENTIAL] were insufficiently informed about the processing and it is not established that they (in freedom) have given permission, [CONFIDENTIAL] has affected this processing to the protection of the personal data of its employees. Considering the nature, seriousness and duration the violation is not a minor violation46, which means that the DPA has imposed a fine reprimand is insufficiently effective, proportionate and dissuasive. That data security was thereby guaranteed does not change this, because [CONFIDENTIAL] the biometric data shouldn't have handled it anyway. The AP is of the opinion that this is a serious violation.

That is why the AP considers the imposition of an administrative fine (which includes both special and general prevention). purpose) is appropriate in this case.

The AP also considers this violation of more than ten months to be of a structural nature, whereby the processing (having the data stored) did not continue until November 2018, but up to and including April 16, 2019. [CONFIDENTIAL] has its own responsibility to comply with the GDPR and that is not taken away by the circumstance that the supervisor sends a signal about unlawful received processing nor by the duration of the AP's investigation.

Secondly, [CONFIDENTIAL] is of the opinion that there was no question of any intent. At the time of the purchasing the software for the finger scans (in 2016), the Protection Act still applied Personal data. [CONFIDENTIAL] states that it is aware of the entry into force of the GDPR on 25 May 2018, but believed that what she was doing was in accordance with the privacy legislation, which was (and is) always confirmed by the supplier.

Referring to section 4.3.2, the AP sees no reason to refrain from it on this basis imposing an administrative fine or reducing the fine amount. As [CONFIDENTIAL] has stated that she was aware of the entry into force of the GDPR and [CONFIDENTIAL] had sufficient time to obtain legal advice, for example. A professional party like [CONFIDENTIAL] may, partly in view of the special nature of the personal data, they are expected to take due care of the applicable standards and comply with them. The AP also notes that the violations

46 See also recital 148 of the GDPR.

prohibition of Article 9(1) GDPR does not require intent as a component. Now that this is one violation, it is not required for the imposition of an administrative fine in accordance with established case law it is demonstrated that there is intent.47 The AP may assume culpability if the perpetrator has been established.48 The perpetrator is not under discussion between the AP and [CONFIDENTIAL], so that culpability is a given.

[CONFIDENTIAL] further argues that the parties involved have not suffered any damage and that the biometric data were secured. The system is set up in such a way that the privacy of the employees is guaranteed. The supplier is ISO 9001 certified and the sub-processor is ISO 9001, ISO 27007, 150 14001 and NEN 7510 certified. The product purchased by [CONFIDENTIAL].

complies with the quality standards according to [CONFIDENTIAL]. Admittedly, it's about
biometric data but the code, which is created on the basis of the fingerprint, is at the discretion
of [CONFIDENTIAL] cannot be traced back to an employee. Immediately after the AP's first visit
[CONFIDENTIAL] has taken measures to stop clocking in/out using
fingerprints and after the second visit by the AP all data was deleted.
The AP does not follow [CONFIDENTIAL]'s view in this either. As mentioned in section 3.1.2, the
AP is of the opinion that with the data stored by [CONFIDENTIAL] natural persons, namely
its employees could be identified. That the biometric data according to
[CONFIDENTIAL] being properly secured is not sufficiently serious in this case, because the violation
does not concern the security of the data, but the not being allowed to process it as such.
[CONFIDENTIAL] further states that clocking in/out by means of fingerprints is direct
after the AP's first visit has stopped, but that does not mean that [CONFIDENTIAL] with the
processing(s) was stopped. After all, according to Article 4, second paragraph, of the GDPR, processing is also -
without being limitative - collecting, recording, organizing, structuring or having stored
facts.
Finally, [CONFIDENTIAL] argues that there are no previous relevant infringements.
In addition, [CONFIDENTIAL] has always cooperated with the AP and has the issue
taken seriously from the outset. [CONFIDENTIAL] also notes that the AP does not rely on any
moment in the process since November 6, 2018, gave the impression that she might be fined
imposed and what the level thereof could be. If [CONFIDENTIAL] was previously by the AP on this
it would have sought advice sooner and taken measures even more quickly. In view of the fact
that [CONFIDENTIAL] was not aware of a possible infringement, she herself did not report it
done or contacted the AP. [CONFIDENTIAL] concludes that of any financial
advantage as a result of the use of the finger scans does not exist.
47 cf. Trade and Industry Appeals Tribunal 29 October 2014, ECLI:NL:CBB:2014:395, par. 3.5.4, Sept. 2, 2015,
ECLI:NL:CBB:2015:312, par. 3.7 and 7 March 2016, ECLI:NL:CBB:2016:54, par. 8.3; Administrative Jurisdiction Division of the

Council of

State 29 August 2018, ECLI:NL:RVS:2018:2879, par. 3.2 and 5 December 2018, ECLI:NL:RVS:2018:3969, par. 5.1.

48 Parliamentary Papers II 2003/04, 29 702, no. 3, p. 134.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

The AP does not follow the view of [CONFIDENTIAL] in this either. Despite the AP not being the same before established an infringement with [CONFIDENTIAL] and according to [CONFIDENTIAL] there is no question of this financial advantage, the AP sees due to the seriousness of the violation and the culpability of [CONFIDENTIAL] no reason to refrain from imposing an administrative fine or to to reduce the fine. The AP refers to paragraphs 4.3.1 and 4.3.2 for the reasons for this. The AP is further believes that the cooperation of [CONFIDENTIAL] has not gone beyond its legal obligation to comply with Article 9, first paragraph, of the GDPR. [CONFIDENTIAL] is not done with that cooperated in a special way with the AP. Finally, the AP notes that during the research phase they cannot comment on the means of enforcement, because then the facts and the report are still being investigated and established. As mentioned earlier, it remains [CONFIDENTIAL]'s own responsibility to research and comply with applicable laws.

In conclusion, the AP sees no reason in [CONFIDENTIAL]'s view to refrain from the imposing an administrative fine or to reduce the fine amount. The AP considers the fine amount to be € 725,000 proportional and there are no other facts and circumstances that necessitate moderation of the aforementioned amount.

4.4 Conclusion

The AP sets the total fine amount at €725,000.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

5. Operative part

fine

The AP submits to [CONFIDENTIAL], due to violation of Article 9, first paragraph, of the AVG a

administrative fine in the amount of €725,000 (in words: seven hundred and twenty-five thousand euros).49

Yours faithfully,

Authority for Personal Data,

e.g.

ir. M.J. Verdier

Vice President

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. For the

submitting a digital objection, see www.autoriteitpersoonsgegevens.nl, under the heading Objection

against a decision, at the bottom of the page under the heading Contact with the Dutch Data Protection Authority. It

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.

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