Confidential/Registered

[CONFIDENTIAL]

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Topic

Decision to impose an administrative fine

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authority data.nl

Dear [CONFIDENTIAL],

The Dutch Data Protection Authority (AP) has decided to pay [CONFIDENTIAL] an administrative fine of €725,000 to be imposed. The AP believes that [CONFIDENTIAL] from May 25, 2018 to April 16, 2019 has the prohibition of Article 9, first paragraph, of the General Data Protection Regulation 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 DPA assesses whether biometric data is being processed, processing responsibility and the violation. In chapter 4 the (height of the) administrative fine and Chapter 5 contains the operative part and the remedies clause.

December 4, 2019

Our reference

[CONFIDENTIAL]

1 Introduction

1.1 Legal entities involved and reason for the investigation

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

On July 5, 2018, the AP received a notification that employees are mandatory at [CONFIDENTIAL] to have their fingerprint scanned. The AP supervisors concluded from the report that employees clock in and out using a fingerprint for time registration. Unpleasant

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 focuses more on the use of the processing of biometric data, such as a fingerprint.

1.2 Process

On September 6 and October 12, 2018, the AP contacted the signaller by telephone to ask questions about his notification about (the obligation to) the use and locations of the finger scan equipment at [CONFIDENTIAL]. As a result, the AP on October 22, 2018 receive documents from the signaller.

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

On March 18, 2019, the AP conducted another investigation at the offices of [CONFIDENTIAL]. The reports on this investigation and the statements made 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 into account this response, the AP has final report adopted. This report is sent by letter dated September 4, 2019 to [CONFIDENTIAL] sent.

In a letter dated September 16, 2019, the AP sent [CONFIDENTIAL] an intention to enforce sent. Also given the opportunity to do so by letter dated 16 September 2019 by the AP, [CONFIDENTIAL] gave its opinion in writing on 21 October 2019 about this intention and the final report on which it is based.

2. Legal framework

2.1 Scope GDPR

Pursuant to Article 2(1) of the GDPR, this Regulation applies to all or part of automated processing, as well as to the processing of personal data that are in a file included or intended to be included therein.

Pursuant to Article 3(1) of the GDPR, this Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, whether or not the processing is carried out in the Union does not take place.

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

1. “Personal data”: any information about an identified or identifiable natural person (“the data subject”); […].

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

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

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

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

2.2 Ban on processing biometric data

Article 9, first paragraph, of the GDPR defines special personal data as follows, insofar as it is relevant here:

“[...] personal data revealing racial or ethnic origin, political opinions, religious or

ideological beliefs, or evidence of 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 a person's sexual behavior or sexual

orientation […]”

Under Article 4(14) of the GDPR, biometric data is personal data that the

are the result of a specific technical processing with regard to the physical, physiological or

behaviour-related 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(1) of the GDPR, the processing of biometric data for the purposes of

uniquely identifying a person is prohibited.

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

second paragraph of the GDPR, insofar as relevant here:

“Paragraph 1 does not apply where any of the following conditions are 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 provides that

the prohibition referred to in paragraph 1 cannot be lifted by the person concerned;

[…]

g) the processing is necessary for reasons of substantial public interest, on the basis of Union law

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

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

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

person concerned;

[...]"

Under Article 4(11) of the GDPR, consent is defined as any free, specific,

informed and unambiguous expression of will with which 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

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

is based on permission. Pursuant to Article 7(3) of the GDPR, the data subject has the right to be

withdraw consent at any time. Before the data subject gives his consent, he is informed of this

notified.

Pursuant to Article 29 of the Implementation Act General Data Protection Regulation (UAVG), attention has been

on Article 9, second paragraph, part g, of the Regulation, the prohibition to use biometric data with the

to process the unique identification of a person does not apply if the processing

necessary for authentication or security purposes.

2.3 Administrative fine

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

under

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

AVG to impose an administrative fine.

2.3.1 GDPR

Pursuant to Article 83(1) of the GDPR, each supervisory authority shall ensure that the
administrative fines imposed under this article for the activities referred to in paragraphs 4, 5 and 6
infringements of this Regulation are effective, proportionate and dissuasive in each case.
Under paragraph 2, administrative fines shall be, according to the circumstances of the
specific case, imposed in addition to or instead of the provisions of Article 58, second paragraph, under a to h and under j,
measures referred to.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

It follows from the fifth paragraph, opening words and under a, that an infringement of the basic principles regarding
processing as in
Article 9 of the GDPR pursuant to paragraph 2 is subject to an administrative fine of up to
€20,000,000 or, for a company, up to 4% of total worldwide annual sales in the previous
financial year, if this figure is higher.

2.3.2 UAVG

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

3. Review

3.1 Processing of biometric personal data

3.1.1 Facts

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

clock in and out [CONFIDENTIAL]. All these scan stations exchange data with a

software program, which, in addition to checking presence and absence, can provide insight into

working hours, absenteeism and overtime.1

[CONFIDENTIAL] has stated that its employees have fingerprints from two fingers

made and recorded. The scanning station calculates a template from the fingerprint and stores it in the

software program. This means that using a photographic scan, unique dots

identified in the lines of the print. The dots together form the basis for a

mathematical calculation to calculate the fingerprint template quality.2

[CONFIDENTIAL] has employee fingerprints recorded as soon as they are hired, so that

one can clock in.3 Statements from the employees of [CONFIDENTIAL] show that they are

called to come by for fingerprinting.4

On March 18, 2019, the AP determined during the investigation at [CONFIDENTIAL] that

[CONFIDENTIAL] has a digital folder containing all fingerprint templates of fingerprints

1 Report of technical investigation during on-site investigation (dated 6 November 2018) dated 12 November 2018, screenshot of website

supplier of January 29, 2019 and report technical investigation including appendices A to H (appendix G (digital content folder bio_templates) and Appendix H (digital photo files) dated 19 March 2019.

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

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

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

of employees ever scanned at [CONFIDENTIAL]. These templates are saved as
text files.5
The AP has established that it can be deduced from the contents of this folder what the period is within which
employee fingerprints are recorded. The fingerprint templates are stored in this folder
as [CONFIDENTIAL] files. The [CONFIDENTIAL] files belong to employees who work in
be employed by [CONFIDENTIAL]. The [CONFIDENTIAL] files belong to former employees
of [CONFIDENTIAL]. When the affected employee's fingerprint templates are
created can be deduced from the date in the individual text files of the templates. In front of
[CONFIDENTIAL] files, the storage date must also match the date of
capture of the fingerprint, which is contained in the text file itself.
The first fingerprint templates were stored on January 23, 2017. From then on, regular
template saved. The last employee fingerprint templates are dated November 8, 2018.
The storage data of the [CONFIDENTIAL] files shows that of 39 employees after May 25, 2018
fingerprint templates were created. It follows from the storage data of the [CONFIDENTIAL] files that after
May 25, 2018 of 31 employees fingerprint templates were created. From the contents of the
[CONFIDENTIAL] files can be deduced that of 17 employees after May 25, 2018
fingerprint templates were created. After 25 May 2018, there will therefore be a total of (39+31+17=) 87 employees
fingerprints captured and stored. The AP has determined that on March 18, 2019, a total of 1,348
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 employees who have had their fingerprints registered and
that were in service on March 18, 2019, the fingerprint templates were actually active in March 18, 2019
the software program and the scan stations.7 The AP has also determined this by means of a staff card
of an employee who was employed at the time. On the relevant staff 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] further stated that of employees who have left employment and as . on March 18, 2019,

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

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

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

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

6 Technical investigation report including appendices A to H (appendix G (digital content map bio_templates) dated 19 March 2019.

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

8 Report technical investigation including appendices A to H, appendix E (printout of file “people in service with finger scan.pptx”) p.

9, of March 19, 2019.

9 Interview with [CONFIDENTIAL] at [CONFIDENTIAL] dated 9 November 2018.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

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

persons who left employment on March 18, 2019.10

The AP took 160 staff card screenshots of employees on March 18, 2019

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

[CONFIDENTIAL] was determined by the number of [CONFIDENTIAL] files in that folder

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

software program and the scan stations.12

Based on the above, the AP concludes that after recording the fingerprint, the templates
of those fingerprints are stored as a text file in a digital folder. These templates from
fingerprints recorded since the beginning of 2017 are therefore still stored there. This also applies
for fingerprint templates of retired employees, although these will then be blocked and
so no longer active in the software program and the scan stations.
Production employees of [CONFIDENTIAL] can only use their
fingerprint and the drop (an identification tag) separately and next to each other and do this
also regularly. Using the template in the software program, their identity is
device attached. It is not possible to conclude from the time registration in the software program whether
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
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 visit of the AP on
November 6, 2018 [CONFIDENTIAL] has stopped scanning the fingerprints of (new)
employees, because it is no longer known whether or not it is allowed.16 On March 18, 2019, the AP has
also found that [CONFIDENTIAL] no more new fingerprints since November 8, 2018
has recorded.
[CONFIDENTIAL] received instructions from the supplier on how to dispose of it on April 16, 2019
of the software and the files contained therein. [CONFIDENTIAL] has stated that they are

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 the file “people employed with finger scan.pptx”),
from March 19, 2019.

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

13 First three interview reports with employees of [CONFIDENTIAL] dated November 7, 2018, interview report with director from [CONFIDENTIAL] dated 9 November 2018, interview report with [CONFIDENTIAL] at [CONFIDENTIAL] dated 9 November
2018 and technical investigation report on site investigation (dated November 6, 2018) dated November 12, 2018.
14 Interview report with director of [CONFIDENTIAL] dated 9 November 2018.
15 Second and third interview report with employees of [CONFIDENTIAL] dated November 7, 2018 and interview report with [CONFIDENTIAL] to [CONFIDENTIAL] dated November 9, 2018.
16 Report of official acts of investigation on the spot at [CONFIDENTIAL] (dated 6 November 2018) of 12 November 2018.

Date
December 4, 2019
Our reference
[CONFIDENTIAL]

subsequently deleted the biometric data of its (former) employees and
log files as evidence for the deletion.17 The log files indicate that
the biometric data has actually been deleted but the exact date on which this happened can be
cannot be inferred from this.18 In view of this, the DPA assumes that the violation will in any case be up to and
continued with April 16, 2019.

3.1.2 Assessment

According to Article 4(1) of the GDPR, personal data concerns 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.

Under Article 4(14) of the GDPR, biometric data includes personal data
which are, inter alia, the result of a specific technical operation with regard to the physical

characteristics of a natural person, on the basis of which unambiguous identification of that natural person is possible or confirmed. Fingerprint data is explicitly mentioned as example of biometric data.

Article 4(2) 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 determined that [CONFIDENTIAL] has fingerprints of 337 (former) employees stored from January 23, 2017 to at least April 16, 2019. As the facts show, these are fingerprints stored as templates and remain stored there even if employees are already off-duty to be. 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 clock out, using the template in the software program to establish their identity confirmed. Thus, just by recording employee fingerprints, further processing of the fingerprint, such as using the fingerprint to enter and exit clocks.

The AP comes to the conclusion that with the data stored by [CONFIDENTIAL] 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 that is confirmed to employees via the finger scanner. Therefore, there is biometric data within the meaning of Article 4(14) 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.

Date

December 4, 2019

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

[CONFIDENTIAL] has digitally stored the fingerprint data and also processes it by using the finger scanning equipment when taking the fingerprint and if employees use their finger scan to be able to clock in and out. The AP comes to the conclusion that [CONFIDENTIAL] as a result has processed (partially) automated biometric data within the meaning of Article 4, part two, of the GDPR.

3.1.3 Conclusion

[CONFIDENTIAL] on May 25, 2018, had stored biometric data of 250 employees who 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 biometrics from May 25, 2018 to April 16, 2019 has processed within the meaning of Article 4(14) of the GDPR.

3.2 Controller

The AP is of the opinion that [CONFIDENTIAL] the purposes and means for the processing of the biometric data. [CONFIDENTIAL] has made the decision to to deploy (and finance) finger-scan equipment as a means to collect biometric data from to process its employees.20

[CONFIDENTIAL] has also determined the purpose of the processing, namely to reduce abuse in clocking in and out for the purpose of time registration. According to [CONFIDENTIAL] and is in the 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 no costs for the purchase, loss or damage of drops.21 Employees also cite the reason that the system offers a conclusive presence registration, that the system with finger scanners

outdated system with drop scanners needs to be replaced and that it can be part in the future

of computer network security (hacking attempts, corporate espionage).22

19 See also Court of Appeal. Amsterdam 12 August 2019, ECLI:NL:RBAMS:2019:6005, which ruled that a fingerprint converted

was based on a code is a (biometric) personal data within the meaning of the GDPR.

20 Interview report with director of [CONFIDENTIAL] dated 9 November 2018, interview report with [CONFIDENTIAL] at [CONFIDENTIAL] of 9 November 2018, overview list and copied documents during on-site investigation (dated 6 November 2018) of 12 November 2018, documents no. 17 and no. 18, and technical investigation report on site investigation (dated 6 November

2018) dated November 12, 2018.

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

on site (dated March 18, 2019) at [CONFIDENTIAL] dated March 19, 2019.

22 Interview report with [CONFIDENTIAL] at [CONFIDENTIAL] dated 9 November 2018 and technical investigation report at on-site investigation (dated November 6, 2018) dated November 12, 2018.

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

as referred to in Article 4(7) of the GDPR.

3.3 Ban on processing biometric data

3.3.1 Introduction

In recent years, the importance of biometrics for the identification of individuals has grown strong

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

processed for the purpose of uniquely identifying a person, including as a special

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, pursuant to Article 9(1) of the GDPR prohibited, unless a legal exception applies.24

In the following, the AP checks whether [CONFIDENTIAL] can successfully invoke for 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 that [CONFIDENTIAL] uses do not include information about the use of fingerprints.25 The employee 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 changes to the production personnel manual. The above paragraph on attendance registration was unchanged has remained.27 In an updated version of the manuals, 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 it have 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 on-site investigation (dated November 6, 2018) of November 12, 2018, no. 3, 4, 5 and 6.

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

and 8.

27 Overview list and copied documents during on-site investigation (dated 6 November 2018) dated 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 interview reports with employees of [CONFIDENTIAL] dated November 7, 2018 and first interview report with employee of [CONFIDENTIAL] dated 19 March 2019.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

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 to process the fingerprints permission is requested from the employees, but that it is a free choice.30

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

The [CONFIDENTIAL] further indicates that there is a possibility to take fingerprints to refuse. The employee concerned must then enter into a discussion with the director. In the in practice this hardly occurs. In the few cases in which this has occurred, the employee has In conversation with the director, he or she still gave his or her fingerprint.32

A [CONFIDENTIAL] has stated that with regard to consent to the employment contract and the personnel manual should be looked at, on the basis of which it deems it to be known to employees that [CONFIDENTIAL] wants to work with fingerprints in the future.33

Regarding the answer to the question of whether permission is requested for the taking of fingerprints, There is a mixed picture among employees in the workplace. 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 verbal consent.34

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

following facts are important.

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

As stated in section 3.1.1. [CONFIDENTIAL] uses a time attendance software program

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

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

scan stations.37

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

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

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

33 Interview report with [CONFIDENTIAL] at [CONFIDENTIAL] dated 9 November 2018.

34 First three interview reports with employees of [CONFIDENTIAL] dated November 7, 2018 and interview reports with

employees of [CONFIDENTIAL] dated March 19, 2019.

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

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

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

[CONFIDENTIAL] dated November 9, 2018.

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

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

finger scan equipment. He took the decision independently in his capacity as general

director of [CONFIDENTIAL].38 As mentioned in section 3.2, the reason for this was the
reducing abuse of clocking in and out for the purpose of time registration. According to there were
[CONFIDENTIAL] also practical benefits. There are no costs for purchase, loss or
damage from droplets. Employees also cite the reason that the system provides a conclusive
attendance registration provides that the finger scanner system replaces the outdated system with drip
scanners need to be replaced and that it may be part of the safety of the
computer network (hacking attempts, corporate espionage). Finally, by using finger identification,
only enter persons who have been trained in the use of advanced equipment.

3.3.3 Assessment

3.3.3.1 Express consent

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

In order for informed consent to be given, the data subject must, among other things, be informed
information 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

A data subject must also be able to freely give consent. In the Guidelines on
consent in accordance with the GDPR is noted in this regard:

“Misrelationship also occurs in the context of the employment relationship. Given the dependence that results from
the employer-employee relationship, it is unlikely that the data subject will give his/her consent to
data processing without fear or real threat of adverse consequences as a result of a
refusal. It is unlikely that the employee would be able to respond freely to a request for consent from
his/her employer for, for example, activating surveillance systems such as camera surveillance in the workplace, or
completing assessment forms, without feeling pressured to give consent. That is 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 should not be the consent of the employees (Article 6(1) under a) because of the nature of the relationship between employer and employee. However, this does not mean that employers never may rely on consent as a legal ground for processing. There may be situations where the employer can demonstrate that consent is actually freely given. Given the mismatch between an employer and its personnel, employees can only give their consent freely in exceptional circumstances, when

38 Interview report with director of [CONFIDENTIAL] dated 9 November 2018, interview report with [CONFIDENTIAL] at [CONFIDENTIAL] dated 9 November 2018 and technical investigation report on site investigation (dated 6 November 2018) of Nov 12, 2018.

39 See Recital 42 of the GDPR, the Guidelines on consent pursuant to Regulation 2016/679 dated 28 November 2017 p. 15 and Article 7(3) of the GDPR.

it has no negative consequences if they do or do not give their consent. […] Mismatches are not limited to government agencies and employees, they can also arise in other situations. Like WP29 in different has emphasized opinions, "consent" can only be valid if the data subject has a real choice and there there is no 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 consent. 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 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.41 To meet the condition of Article 9(2)(a) of the GDPR for exception

the prohibition of processing of biometric data in Article 9(1) 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 GDPR Consent Guidelines, express
consent to the way in which consent is expressed by the data subject. Hereby
According to the Guidelines, this may include written consent, signature (possibly
with electronic signature), the sending of an e-mail by the data subject or consent with
two-step verification. In theory, the use of oral statement may also be sufficient to establish valid
to obtain explicit consent, however, it may be difficult for the controller to
proof that all conditions for valid
express permission.42
On the basis of the following facts, the AP comes to the conclusion that [CONFIDENTIAL] has not
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. Section 3.3.2 shows
after all, with [CONFIDENTIAL] no documentation of policies or procedures for or evidence of the
granting permission for the recording of fingerprints and refusal thereof. Thereby
several employees stated that fingerprint scanning was mandatory and that
permission is not requested for this, not even in the context of signing the
employment contract or receipt of the employee handbook. Two employees stated that
40 Guidance on consent pursuant to Regulation 2016/679 dated 28 November 2017, pp. 7-8. Last revised
and adopted by the Article 29 Working Party on Data Protection on April 10, 2018.
41 Guidelines on consent pursuant to Regulation 2016/679 dated 28 November 2017, p. 23.

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

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

they have given verbal consent for the recording of their fingerprint.

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

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

employees have express consent within the meaning of Article 9(2)(a) of the GDPR

for the processing of their biometric data.

Superfluously, the AP notes that [CONFIDENTIAL] has also not been able to demonstrate that her

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

freedom to give 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

has to clock in completely with the fingerprint. In the most recent employee handbook of

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

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

recording the fingerprints was not announced and that they have no information about this

receive.

In addition, [CONFIDENTIAL] has not demonstrated that any permissions given are freely

its employees have been 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 freedom of choice for employees was to choose whether or not to clock in and out using their fingerprint – different employees have experienced it as an obligation to have their fingerprint registered. Between the employer and employee, there is a hierarchical relationship. Given the dependency that arises from the employer-employee relationship, it is unlikely that the employee or freely give its consent. Moreover, [CONFIDENTIAL] has not demonstrated that in in this case, freely consent has been given.

[CONFIDENTIAL] must demonstrate pursuant to Article 7(1) of the GDPR 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 the above, the AP is of the opinion that [CONFIDENTIAL] has not been able to demonstrate that her employees have express consent within the meaning of Article 9(2)(a) of the GDPR for the processing of their biometric data.

Opinion [CONFIDENTIAL] and response AP

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

had been talking about putting the finger scan system into use and had only good intentions in doing so. It has also never been an obligation to clock in and out with the finger scan; this was always possible still with the drop. [CONFIDENTIAL] is therefore of the opinion that the employees are free to were able to give 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 present drop clocks, 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 and to have stopped clocking in and out using fingerprints. after that date, no fingerprints are recorded anymore. After the AP's second visit on March 18, 2019 [CONFIDENTIAL] has contacted the supplier of the fingerprint equipment and the taken fingerprints and leave the fingerprint registration program remove. [CONFIDENTIAL] wanted to ensure that all biometric data destroyed so that [CONFIDENTIAL] would not be exposed to 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] believes that the employees freely have given permission for the processing of the fingerprints. The AP follows the view of [CONFIDENTIAL]. Given the dependency that results from the relationship between employer and employee, it is unlikely that the employee will be able to freely give his or her consent. If in this exceptional case there was free consent, [CONFIDENTIAL] would have have to demonstrate. [CONFIDENTIAL] has provided no evidence that its employees consent have given for the processing of the fingerprints, let alone that the consent is free and has been informed. Moreover, 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 registered.

3.3.3.2 Necessary for authentication or security purposes

Article 9(2)(g) of the GDPR allows for an exception in national law to the

prohibition to process biometric data for reasons of substantial public interest. In
The Netherlands has given substance to this in Article 29 of the UAVG, by processing biometric data
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 exception for the processing of biometric data. Furthermore, it says here:
“A consideration must be made as to whether identification with biometric data is necessary for
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 be done 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 access to a repair shop garage,
the need for security will not be such that employees can only gain access with biometrics and
to this end, these data are recorded in order to exercise access control. On the other hand, biometrics can sometimes
are an important form of security for, for example, information systems, which themselves contain a lot of personal data
containing illegal access, including by employees, must be prevented. In order to make this assessment possible
in circumstances in which consent cannot be given freely, is a provision in the bill
which allows 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 as to whether identification by means of
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 this must be done with biometric data

find. This is subject to a strict test. For example, biometrics may be used at a nuclear power plant for access control. There the importance of security is very great and only certain people are allowed have access. [CONFIDENTIAL] should also have considered whether the processing of fingerprints of employees at [CONFIDENTIAL] is proportional. The use of biometric personal data when accessing, for example, the garage of a repair company, this key cannot be used to endure. After all, the need for security is then not so great that people can use should be able to access biometrics. In addition, security can also be used in other less far-reaching ways.

As stated in section 3.3.2, the business activities of [CONFIDENTIAL] include: [CONFIDENTIAL]. [CONFIDENTIAL] according to [CONFIDENTIAL] simple work is performed, such as [CONFIDENTIAL]. According to [CONFIDENTIAL], [CONFIDENTIAL] also works with advanced equipment to make them.

[CONFIDENTIAL] uses the relevant software program for time attendance and – based on thereof – the administration of salary, leave and illness. The presence of employees in the past only registered by means of clocking in and out with drops at scan stations. The director of [CONFIDENTIAL] has independently decided to expand the time registration system with the finger scanning equipment. As stated in section 3.2, the reason for this was the reduction of abuse in clocking in and out for the purpose of time registration. According to [CONFIDENTIAL] there were also practical benefits. There are no costs for purchasing, losing or damaging drops.

Employees also cite the fact that the system offers a conclusive attendance registration as a reason the finger scanner system is to replace the obsolete drip scanner system 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 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 (the prevention of misuse of) time registration, attendance control and authorized use of equipment at [CONFIDENTIAL] is not necessary and proportionate. The previously described activities at [CONFIDENTIAL], including [CONFIDENTIAL], rather approach the work within a garage of a repair company, whereby 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 (preventing misuse of) time registration, but given this purpose and the business activities of [CONFIDENTIAL] that interest does not justify an exception to the prohibition of 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 access biometrics and this data must be recorded for this purpose to exercise access control. In addition, other ways that are less infringing on the make employees' privacy, also make it happen.

[CONFIDENTIAL] has indicated that it agrees on the draft report of the findings of the AP with the AP that the ground for exception 'necessary for security or authentication' [CONFIDENTIAL] may not work. According to [CONFIDENTIAL], this is the main reason for [CONFIDENTIAL] Stop using biometrics for access control.

[CONFIDENTIAL] has not expressed an opinion on the final report of this exception ground.

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 to justify security purposes. [CONFIDENTIAL] may be concerned with the processing of

fingerprints therefore do not invoke the exception option of Article 9, second paragraph, under

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

3.3.4 Conclusion

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

process. The AP concludes that the processing of biometric data is

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

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] has violated the prohibition of Article 9, first paragraph, of the

violate GDPR.

3.4 Final conclusion

The AP concludes that [CONFIDENTIAL] as controller of May 25, 2018

up to and including 16 April 2019, has violated the prohibition of Article 9(1) of the GDPR by using biometrics

process the data of its employees.

4. Fine

4.1 Introduction

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

violate the GDPR by processing biometric data of its employees.

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

to impose a fine on the basis of Article 58, second paragraph, preamble and under i and Article 83, fifth paragraph, of the

GDPR, read in conjunction with Article 14(3) of the UAVG. The AP uses the

Fines Policy Rules 2019.44

After this, the AP will first briefly explain the penalty system, followed by the motivation of the

fine in the present case.

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

Pursuant to Article 58, second paragraph, preamble and under i and Article 83, fifth paragraph, of the GDPR, read in in connection with article 14, third paragraph, of the UAVG, the AP is authorized to [CONFIDENTIAL] in the event of to impose an administrative fine up to € 20,000,000 or . for a violation of Article 9, first paragraph, of the GDPR up to 4% of total worldwide annual turnover in the previous financial year, whichever is higher.

The AP has established Fine Policy Rules 2019 regarding the interpretation of the aforementioned power to imposing an administrative fine, including determining the amount thereof.45

Pursuant to Article 2, under 2.2, of the 2019 Fine Policy Rules, the provisions with regard to violation of which the AP can impose an administrative fine not exceeding the amount 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 higher, classified in Annex 2 as Category I, Category II, Category III or Category IV. The fine 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 statutory 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 Stcrt. 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 (up 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 basic fine will be

increased or decreased depending on the extent to which the factors referred to in Article 7 to that end

give rise to.

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

(Awb) taking into account the factors derived from Article 83, second paragraph, of the GDPR and in the

Policy rules mentioned under a to k:

the nature, seriousness and duration of the infringement, taking into account the nature, scope or purpose of the infringement

processing in question as well as the number of data subjects affected and the extent of the damage suffered by them

injury;

b. the intentional or negligent nature of the infringement;

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

limit damage;

d. the extent to which the controller […] is responsible given the technical and

organizational measures that he has carried out in accordance with Articles 25 and 32 of the GDPR;

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

f. the extent to which there has been cooperation with the supervisory authority to remedy the breach and

limit the possible negative consequences thereof;

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

h. the manner in which the supervisory authority became aware of the infringement, in particular whether, and

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

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

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

matter have been taken;

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

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

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

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

result.

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

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

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

factors give rise to this, the fine bandwidth of the next higher or the next

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

on the basis of Article 5:46, second paragraph, of the Awb, to what extent the offender can be blamed for this.

4.3 Fine amount

4.3.1. Nature, seriousness and duration of the infringement

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

the seriousness and duration of the infringement. In its assessment, the AP takes into account, among other things, the nature,

the

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

suffered damage to them.

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

Personal data that are particularly sensitive deserve specific protection, because the processing
can pose high risks to fundamental rights and freedoms. Those involved serve
therefore have a high degree of control over their biometric data. The starting point is therefore that it
processing of special personal data is in principle prohibited. There is only a limited number of
and exceptions laid down in the GDPR are possible. With fingerprinting and the
then storing biometric data [CONFIDENTIAL]x in this case has the high
level of protection offered by Article 9(1) of the GDPR has been infringed.
[CONFIDENTIAL] has biometric data of her from May 25, 2018 to April 16, 2019.
employees processed. This violation therefore took place in a structural manner and for a
continued for a longer period of time. During this period, [CONFIDENTIAL] also has the biometric
data of former employees, while there was no need for this. During this
During this period, the data subjects therefore had no control over their biometric data.
On the one hand, [CONFIDENTIAL] has encrypted the biometric data and stated that only a
limited number of people had access to the data. On the other hand, it is apparent from 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 infringement.
In view of the fact that the violation lasted more than ten months in which 337 were involved
affected, there has been a serious situation. [CONFIDENTIAL] not only has the
biometric data of current employees but also of former employees without necessity
kept for a longer period of time. In addition, the employees were insufficiently informed about the processing and
it is not certain that they (freely) gave their consent, as a result of which, in the opinion of the
AP there is a serious violation in which the special data of those involved are incorrectly
conditions have been processed.
As a result, a large group of [CONFIDENTIAL] employees did not know for which
purposes the fingerprints were used and that they could give their consent at any time
moving in. As a result, those involved have had no control over what happened to them for a longer period of time

biometric data was done at [CONFIDENTIAL]. And it is precisely this control that the GDPR imposes on
wants to offer data subjects, so that data subjects are able to protect their personal data and
to surrender in freedom. Therefore, the AP is of the opinion that there is a serious violation,
but sees no reason in this case to increase or decrease the amount of the fine.

4.3.2 Blame

Pursuant to Article 5:46, second paragraph, of the Awb, when imposing an administrative fine, the AP
into account the extent to which this can be blamed on the offender.

Pursuant to Article 9(1) of the GDPR, it is in principle prohibited to collect biometric data
process. The GDPR applies from 25 May 2018 and dates from 27 April 2016.
Data controllers have had two years until May 25, 2018 to
processing activities in accordance 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 trusted that
would inform this professional party [CONFIDENTIAL] of any changes. The AP belongs to
judge that this circumstance does not exculpate [CONFIDENTIAL]. The starting point is that
[CONFIDENTIAL] has its own responsibility to act as soon as the entry into force of the
GDPR to comply with the rules set out therein. [CONFIDENTIAL] has failed to self-process
of the biometric data against the GDPR or to obtain legal advice about this. Instead
[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 thoroughly ascertains and complies with the standards that apply to it. [CONFIDENTIAL] has its actions violated the high level of protection for special personal data. The AP considers this culpable.

4.3.3 Opinion [CONFIDENTIAL] and AP . response

[CONFIDENTIAL] argues in its view that on the basis of the factors of Article 83, paragraph 2 of the GDPR and the Guidelines for the application and establishment 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 puts the points from the view of [CONFIDENTIAL] below briefly, with a response from the AP.

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

[CONFIDENTIAL] used for the collection and processing of the fingerprints of a professional company and a professional program, where the security of the data is guaranteed and has not been used for any other purpose. The parties involved have [CONFIDENTIAL] also suffered no damage and will not suffer any damage, now that the relevant data have since been destroyed. In addition, the number of people involved is limited according to

[CONFIDENTIAL], now that it concerns employees of [CONFIDENTIAL] in the period January 2017 to November 2018. Immediately after the first visit of the AP, [CONFIDENTIAL] stopped collecting of fingerprints and after the second visit in March 2019, [CONFIDENTIAL] ensured that all relevant data was destroyed. Incidentally, [CONFIDENTIAL] notes with regard to the last, that the AP already on July 5, 2018 (just a good month after the GDPR came into force) received a notification about the finger scans. The AP's first investigation was not until November 6. 2018 and the second examination on March 18, 2019. If [CONFIDENTIAL] earlier, that is, immediately after the notification (when the GDPR had just come 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 its employees' biometric data. By doing so, [CONFIDENTIAL] Violated the essence 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 consent, [CONFIDENTIAL] has prejudiced this processing to the protection of the personal data of its employees. Given the nature, seriousness and duration of the violation, there is no question of a minor infringement46, as a result of which the AP has imposed a deems the reprimand insufficiently effective, proportionate and dissuasive. That the security of the data was guaranteed does not affect this, because [CONFIDENTIAL] the biometric data shouldn't have handled it anyway. The AP believes that this is a serious violation.

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

The AP also finds this violation of more than ten months a violation of a structural nature, whereby the processing (having stored the data) 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 deprived of the circumstance that the supervisor sends a signal about unlawful processing, nor due to the duration of the DPA's investigation.

Secondly, [CONFIDENTIAL] is of the opinion that there was no intent. At the time of the purchase of the software for the finger scans (in 2016), the Protection Act was still in force Personal data. [CONFIDENTIAL] states that it is aware of the entry into force of the GDPR on 25 May 2018, but was under the impression that what she did 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 waive the decision on this basis imposing an administrative fine or reducing the amount of the fine. As [CONFIDENTIAL] has stated she was aware of the entry into force of the GDPR and had [CONFIDENTIAL] sufficient time to obtain legal advice, for example. From a professional party such as [CONFIDENTIAL] may, also in view of the special nature of the personal data, it is expected that they are fully aware of the verify and comply with applicable standards. The AP further notes that the violations

46 See also recital 148 of the GDPR.

prohibition of Article 9(1) GDPR does not require intent as an element. Now that this is a violation, the imposition of an administrative fine in accordance with established case law does not require that it is demonstrated that there is intent.47 The DPA may presume culpability if it offense is established.48 Perpetration is not up for discussion between the AP and [CONFIDENTIAL], so that culpability is a given.

[CONFIDENTIAL] further argues that the data subjects suffered no harm and that the biometric data was 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]

thus complies with the quality standards according to [CONFIDENTIAL]. Although it is about
biometric data but the code, which is created on the basis of the fingerprint, is in the opinion
of [CONFIDENTIAL] cannot be traced back to an employee. Immediately after the first visit of the AP
[CONFIDENTIAL] has taken action to stop clocking in/out using
fingerprints and after the second visit of the AP all data has been deleted.
The AP does not follow the view of [CONFIDENTIAL] in this either. As stated 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] were properly secured in this case is insufficiently serious, because the violation
does not refer to the security of the data but to not being allowed to process it as such.
[CONFIDENTIAL] further states that clocking in/out using fingerprints is direct
has stopped after the first visit of the AP, but that does not mean that [CONFIDENTIAL] with the
processing(s) was discontinued. After all, according to Article 4, second paragraph, of the GDPR, processing is also -
without being limitative - collecting, recording, organizing, structuring or having stored
data.
Finally, [CONFIDENTIAL] argues that there are no previous relevant infringements.
[CONFIDENTIAL] has also always cooperated with the AP and has resolved the matter
taken seriously from the start. [CONFIDENTIAL] notes hereby that the AP does not in any way
moment in the process since November 6, 2018, has given the impression that she might be fined
impose and what the amount could be. If [CONFIDENTIAL] was previously by the AP on this
pointed out, it would have sought advice earlier and taken measures even more quickly. In view of the fact
that [CONFIDENTIAL] was not aware of a possible infringement, it did not report itself
done or contacted the AP. [CONFIDENTIAL] concludes that any financial
there is no benefit as a result of using the finger scans.
47 cf. Trade and Industry Appeals Tribunal 29 October 2014, ECLI:NL:CBB:2014:395, para. 3.5.4, September 2, 2015,
ECLI:NL:CBB:2015:312, para. 3.7 and 7 March 2016, ECLI:NL:CBB:2016:54, para. 8.3; Administrative Jurisdiction Division of

the Council of

State 29 August 2018, ECLI:NL:RVS:2018:2879, para. 3.2 and 5 December 2018, ECLI:NL:RVS:2018:3969, para. 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. Even though the AP hasn't been the same before has established an infringement with [CONFIDENTIAL] and according to [CONFIDENTIAL] there is no question of 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] did not go beyond its legal obligation to comply with Article 9(1) of the GDPR. [CONFIDENTIAL] does not stop there cooperated in a special way with the AP. Finally, the AP notes that during the investigation phase, it cannot express themselves about the means of enforcement, because then the facts and the report will still be investigated and established. As mentioned earlier, it remains the sole responsibility of [CONFIDENTIAL] to investigate and comply with applicable laws.

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

4.4 Conclusion

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

Date

December 4, 2019

Our reference

[CONFIDENTIAL]

5. Operative part

fine

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

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

Yours faithfully,

Authority Personal Data,

w.g.

ir. M.J. Verdier

Vice President

Remedies Clause

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

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

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

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

The address for submission on paper is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ Den Haag.

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

In your notice of objection, write at least:

- your name and address;

- the date of your notice of objection;

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

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

- your signature.

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