Summary of research [CONFIDENTIAL]

The Dutch Data Protection Authority (AP) has fined the company [CONFIDENTIAL] of

725,000 euros for the unlawful taking of fingerprints from its employees and the use

of finger scans. In this summary of the investigation you can read how the AP came to this decision.

Reason for the investigation

On July 5, 2018, the AP received a notification that employees are mandatory at [CONFIDENTIAL]

to have their fingerprint scanned. [CONFIDENTIAL]. The report revealed that employees at

[CONFIDENTIAL] Had to clock in and out using a fingerprint.

In response to this signal, the AP launched an investigation at the end of October 2018 into compliance by

[CONFIDENTIAL] of Article 9 of the General Data Protection Regulation (GDPR). This article

This includes the ban on the processing of biometric data, such as fingerprints. The

AP therefore conducted an on-site investigation at [CONFIDENTIAL].

Why did the AP pick this up?

Ensuring the privacy of an individual is of great importance when using biometrics.

Biometric data, such as a fingerprint, are special personal data within the meaning of

Article 9 GDPR. These are personal data that are, by their nature, particularly sensitive because the processing

could pose significant risks to the fundamental rights and freedoms of

people. Unique body characteristics such as a fingerprint can also be traced back to one individual.

Biometric data also often contain more information than is strictly necessary for, for example,

identification.

The processing of biometric personal data deserves specific protection. By virtue of Article

9 GDPR, the processing of biometric data is therefore prohibited, unless one of the exhaustive

listed exceptions to Article 9(2) of the GDPR arise.

Actual findings of the study

According to [CONFIDENTIAL], the reason for introducing the finger scanning equipment was the

reducing abuse when clocking in and out. In addition, there would be practical advantages. Like

the fact that there is no cost to employees for the purchase, loss or damage of a
'drop', which can also be used to clock in and out at [CONFIDENTIAL]. Other reasons for it
input of the finger scanning equipment were that this system provides a conclusive attendance registration
offers that the finger scanner system was to replace the outdated droplet scanner system
and that it could address security risks in the future.
[CONFIDENTIAL] uses the finger scan software for attendance and time registration and – based on
thereof – for payroll administration. The drops and the finger scan can be used side by side
used. Employees are therefore not obliged to clock in or out with their fingerprint.
Employees need at least two fingerprints to scan their fingerprints
have to hand over. After capturing the fingerprint, the templates of those fingerprints
saved as text file. These fingerprint templates have been saved. Since the introduction of
the system in 2017, fingerprint templates of a total of 337 employees were stored and these are not
removed upon termination of employment.
No information was included in the employment contract about the use of fingerprints.
Employees were only informed through the July 2017 employee handbook that
[CONFIDENTIAL] intended to fully clock in with the fingerprint. for many
employees, the recording of a fingerprint came as a surprise.
Furthermore, [CONFIDENTIAL] did not have any policies, procedures or other documentation by which it
were able to demonstrate that they requested explicit permission to take fingerprints and
using the finger scans. No evidence was also found that employees gave permission for this
had given or refused. Employees only sign for receipt of a drop.
Some employees indicated that having the fingerprint scanned was mandatory and that there was no
permission was requested. Two employees indicated that they had verbal consent
have given. Some employees also indicated that if they refused to give the fingerprint,
having it scanned, a conversation with the director / board followed, after which (almost) everyone in practice
had his/her fingerprint scanned.

The finger scan equipment has been active at [CONFIDENTIAL] since the beginning of 2017. The first fingerprint templates were captured and stored on January 23, 2017. From then on, templates saved regularly. The latest captured and saved fingerprint templates from employees date from November 8, 2018. From early 2017 to May 25, 2018 there are 250 employees fingerprints captured and stored. In the period after the introduction of the GDPR (from 25 May 2018) until November 8, 2018, fingerprints of even more employees have been recorded and stored. In in total that comes to 337 (former) fingerprints. Since November 8, 2018 [CONFIDENTIAL] stopped recording and therefore also storing the fingerprints of new employees.

If an employee leaves employment, his/her data and fingerprint templates will be retained, but blocked in the software program. On March 18, 2019, the AP found that the fingerprint templates of employees who have had their fingerprint registered and who have were currently employed, were active in the software program and scan stations, so that they fingerprint clock in and out. These templates of fingerprints that have been used since early 2017 recorded, were therefore still kept there. This also applies to fingerprint templates from employees who are out of service, although they are then blocked and therefore no longer active in the software program and the scan stations. [CONFIDENTIAL] has at least until April 16, 2019 the fingerprint templates of its (former) employees. Just after that, [CONFIDENTIAL] deleted the stored fingerprint templates of all its (former) employees from the systems and log files provided as justification for this.

Assessment of the facts

According to Article 4(14) of the GDPR, biometric data includes personal data that, among other things, result of a specific technical processing of the physical characteristics of a natural person. And on the basis of which unambiguous identification of that natural person is or will be possible confirmed. Fingerprint data is explicitly mentioned as an example of biometric data data.

Biometric data is special personal data pursuant to Article 9(1) of the GDPR. The processing
of special personal data is prohibited in principle on the basis of Article 9(1) of the GDPR. The ban is
does not apply if one of the grounds for exception to the
processing ban has been complied with. The first exception relevant to this case is stated in Article 9 paragraph
2(a) GDPR . The second possibility of exception follows from Article 9(2)(g) GDPR which is further
completed by the Dutch legislator in Article 29 of the GDPR Implementation Act. It concerns processing on
under “explicit consent” or that are “necessary for authentication or security purposes”
to be.

Exception: express consent

Under Article 4(11) GDPR, consent is a free, specific, informed and
unambiguous expression of will by which someone makes a statement or an unambiguous active act
accepts a processing of his/her personal data.

Explicit consent is required in certain situations where there is a serious risk of
data protection occurs. And where a high level of individual control over
personal data is appropriate. The term "explicit" refers to the way in which consent is given by the
concerned persons. It means that someone has an express statement of consent
must give. For example, written permission, signing, sending an email to
consent or consent with two-factor authentication.

[CONFIDENTIAL] did not have any policies, procedures, or other documentation that would allow them to
demonstrate that they have requested express permission to take fingerprints and
using the finger scans. No evidence was also found that employees gave permission for this
had given or refused. Employees are only through the July employee handbook
2017 informed that [CONFIDENTIAL] had the intention to go completely with the fingerprint
clock in. An investigation by the AP has shown that recording the fingerprints was not
announced to the employees and that they have not received any information about this.

In addition, several employees stated that scanning the fingerprints was mandatory

and that permission is not requested. Not even in the context of the signing of the
employment contract or receipt of the employee handbook. [CONFIDENTIAL] has not
demonstrated that its employees were sufficiently informed about the processing of the biometric
data, nor that its employees have given (explicit) permission for the processing
of their biometric data.
Even if there was consent, it would also have to be 'freely given'.
This means that there should be no coercion behind it or that consent is a condition for anything else.
However, employees indicated that fingerprint scanning was mandatory. Also have
some employees indicated that in case of refusal to have the fingerprint scanned, a conversation with
the director/board followed, after which (almost) everyone had their fingerprint scanned in practice.
Despite the fact that [CONFIDENTIAL] believes that there was freedom of choice for employees to decide whether or not to
and clock out using their fingerprint, several employees have it as a
experience an obligation to have their fingerprint registered. Given the dependence that results
of the employer-employee relationship, it is unlikely that the employee will
consent freely. Moreover, [CONFIDENTIAL] has not shown that in this
case freely given permission. For this reason, any permission is given from the
employees of [CONFIDENTIAL] as not freely given.

The derogation option from Article 9(2)(a) GDPR to the prohibition of processing
biometric data on the basis of the explicit consent of the data subject therefore goes in this case
not on.
Necessary for authentication or security purposes
The processing of biometric data could further be allowed if necessary
for authentication or security purposes. To do this, a decision must be made as to whether
identification by means of biometrics is necessary and proportional for authentication or
security purposes. The AP is of the opinion that the processing of biometric data in the context of

of (preventing misuse of) time registration, attendance control and authorized use of
equipment at [CONFIDENTIAL] is not necessary and proportional. For the work at
[CONFIDENTIAL], [CONFIDENTIAL], the need for security is not so high that
employees must be able to access biometrics and this data must be recorded for this purpose
to exercise access control. In addition, other less intrusive ways, this also
accomplish. [CONFIDENTIAL] can therefore not interfere with the processing of fingerprints
invoke the derogation option provided for in Article 9(2)(g) of the GDPR in conjunction with Article 29
UAVG.
Processing fingerprints without one of the exhaustively listed exceptions of
applies, leads to a violation of Article 9 GDPR. Based on the findings of the investigation
it is concluded that with [CONFIDENTIAL] special personal data, namely biometric
data of employees has been processed. It has not been found that any of the grounds for exception in
Article 9 (2) GDPR occurs. In doing so, [CONFIDENTIAL] acts in violation of the ban
Article 9 (1) GDPR.
Sanction
[CONFIDENTIAL] has the prohibition of Article 9(1) GDPR from 25 May 2018 to 16 April 2019
by processing biometric data of its employees. The AP explains for this
violation to [CONFIDENTIAL] a fine of € 725,000 on the basis of Article 58, paragraph 2, opening words
and under i and Article 83(5) GDPR, read in conjunction with Article 14(3) GDPR.