Study summary [CONFIDENTIAL]

The Dutch Data Protection Authority (AP) has imposed a fine of [CONFIDENTIAL] on the company 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 at [CONFIDENTIAL] are required to have their fingerprint scanned. [CONFIDENTIAL]. The report showed that employees at [CONFIDENTIAL] had to clock in and out using a fingerprint.

At the end of October 2018, the AP started an investigation into compliance by this signal [CONFIDENTIAL] of Article 9 of the General Data Protection Regulation (GDPR). This article concerns, among other things, the ban on the processing of biometric data, such as a fingerprint. The AP therefore conducted an on-site investigation at [CONFIDENTIAL].

Why did the AP take 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 in the sense of Article 9 GDPR. These are personal data that are, by their nature, particularly sensitive because of the processing may pose significant risks to the fundamental rights and freedoms of people. Moreover, unique body characteristics such as a fingerprint can be traced back to one individual. Biometric data also often contain more information than is strictly necessary for e.g 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 of Article 9 (2) GDPR occur.

Factual findings of the investigation

According to [CONFIDENTIAL], the reason for introducing the finger scanning equipment was it reducing abuse when clocking in and out. In addition, there would be practical benefits. As

the fact that there are no costs for the 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
introduction of the finger-scan equipment were that this system provides a comprehensive attendance registration
that the system with finger scanners had to replace the outdated system with drop scanners
and that it could address security risks in the future.
[CONFIDENTIAL] uses the fingerprint software for attendance and time registration and – based
of which – for payroll administration. The drops and the finger scan can be placed next to each other
used. Employees are therefore not obliged to clock in or out with their fingerprint.
Employees must have prints of at least two fingers before scanning their fingerprint
have to issue. After capturing the fingerprint, the templates of those fingerprints are available
saved as a text file. These templates of fingerprints have been preserved. Since the introduction of
fingerprint templates of a total of 337 employees are stored in the system in 2017 and are not
removed upon termination of employment.
The employment contract did not contain any information about the use of fingerprints.
Employees were only informed about this via the July 2017 employee handbook
[CONFIDENTIAL] intended to clock in completely with the fingerprint. For many
employees, recording a fingerprint therefore came as a surprise.
Further, [CONFIDENTIAL] had no policies, procedures or other documentation with which it
could demonstrate that they requested explicit permission to take fingerprints and
using the finger scans. Also, no evidence was found that employees gave permission for this
given or refused. Employees only sign for receipt of a drop.
Some employees indicated that having the fingerprint scanned was mandatory and there was none
permission was requested. Two employees have indicated that they have verbal consent
have given. Some employees have also indicated that if they refuse to provide the fingerprint
had it scanned, a meeting with the director/board followed, after which (almost) everyone in practice
had his/her fingerprint scanned.

The fingerprint equipment has been active at [CONFIDENTIAL] since early 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 were captured and stored. In in total this 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 fingerprints recorded and those on that were currently employed were active in the software program and scan stations, so that they could use their fingerprint could clock in and out. These templates of fingerprints 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 are 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 afterwards [CONFIDENTIAL] the stored fingerprint templates of all its (former) employees are removed from the systems and log files provided to substantiate this.

Assessment of the facts

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

Biometric data are special personal data pursuant to Article 9 (1) GDPR. The processing
sensitive personal data is in principle prohibited under Article 9 (1) GDPR. The ban is
does not apply if one of the grounds for derogation from the
processing ban has been met. The first exception relevant to this case is stated in Article 9, paragraph
2 (a) GDPR . The second exception possibility follows from Article 9 (2) (g) GDPR, which is further on
completed by the Dutch legislator in Article 29 of the AVG Implementation Act. It concerns processing on
on the basis of 'explicit consent' or which is 'necessary for authentication or security purposes'
are.
Exception: express consent
Under Article 4(11) GDPR, consent is free, specific, informed and
unambiguous expression of will with which someone with a statement or an unambiguous active act
accepts processing of his/her personal data.
Explicit consent is required in certain situations where there is a serious risk
data protection occurs. And involving a high level of individual control over it
personal data is appropriate. The term "explicit" refers to the way consent is given by the
persons involved. It means that someone has an explicit statement of consent
must give. For example, written permission, signing, sending an e-mail to
consent or consent with two-factor authentication.
[CONFIDENTIAL] had no policies, procedures, or other documentation with which to do so
demonstrate that they requested explicit permission to take fingerprints and the
using the fingerprint scanner. Also, no evidence was found that employees gave permission for this
given or refused. Employees are only through the July employee handbook
2017 informed that [CONFIDENTIAL] intended to go full-fingerprint
clock in. An investigation by AP has shown that the recording of 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 no permission is requested for this. Not even in the context of signing 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 consent were indeed given, 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 something else.
However, employees indicated that fingerprint scanning was mandatory. Also have
some employees indicated that if they refuse to have their fingerprints scanned, a conversation with
the director/board followed, after which (almost) everyone had their fingerprint scanned in practice.
Although [CONFIDENTIAL] believes that there was a freedom of choice for employees whether or not to
and clocking out using their fingerprint, several employees have it as one
experience an obligation to have their fingerprints recorded. Given the dependency that results
of the relationship between employer and employee, it is unlikely that the employee will be his or her
consent freely. Furthermore, [CONFIDENTIAL] has not shown that in this
case free consent has been granted. For this reason, any consent given by the
employees of [CONFIDENTIAL] as not freely given.

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

of (preventing abuse of) time registration, attendance control and authorized use of equipment at [CONFIDENTIAL] is not necessary and proportionate. For the work at [CONFIDENTIAL], [CONFIDENTIAL], the need for security is not so great 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 less drastic ways can also do this to accomplish. [CONFIDENTIAL] can therefore not act with regard to the processing of fingerprints invoke the possibility of derogation of Article 9(2)(g) GDPR in conjunction with Article 29 UAVG.

Processing fingerprints without any of the exhaustively listed exceptions 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 are processed. It has not been shown that any of the grounds for exemption in Article 9 (2) GDPR occurs. In doing so, [CONFIDENTIAL] is acting in violation of the prohibition Article 9 (1) GDPR.

Sanction

[CONFIDENTIAL] has from 25 May 2018 to 16 April 2019 the prohibition of Article 9 (1) GDPR violated by processing biometric data of its employees. The AP submits for this infringement to [CONFIDENTIAL] a fine of € 725,000 on the basis of Article 58, paragraph 2, opening words and under i and Article 83 paragraph 5 GDPR, read in conjunction with Article 14 paragraph 3 UAVG.