Use of fingerprints for access control

Date: 08-07-2020

Decision

Private companies

In a specific case, it is not against the rules for a company to process fingerprint information for the purpose of uniquely identifying employees.

Journal number: 2019-31-1650

Summary

The Danish Data Protection Agency has made a decision in a case where a trade union on behalf of one of the association's members has complained that a company processes information about fingerprints with a view to unambiguously identifying which employee is approaching and leaving the workplace.

The company stated that this was a control measure which had been notified in accordance with the DA / LO agreement on control measures.

The company justified the control measure on the grounds that it is crucial for food safety, including the company's export opportunities, that unauthorized persons do not gain access to the production and that it can be identified at any time who has participated in the production of a given product. Key tags that employees scan do not provide sufficient assurance that it can be unambiguously identified who has been present in the production, as there may be theft of key tags or replacement of key tags both incorrectly and intentionally.

After an overall review, the Danish Data Protection Agency found that there was no basis for overriding the company's assessment. The processing could therefore take place within the framework of the data protection rules.

Decision

The Danish Data Protection Agency hereby returns to the case where [Trade Union A], on behalf of […] (complainants), has contacted the Authority about [Company B] 'processing of personal data.

[Company B] has in the case been represented by Danish Industry.

The Danish Data Protection Agency has understood the inquiry as a complaint that [Company B] processes information about complaints in the form of information about his fingerprints in connection with an introduced control measure in accordance

with the DA / LO agreement on control measures.

Decision

The Danish Data Protection Agency finds - after the matter has been dealt with at a meeting of the Data Council - that [Company B] ’s processing of information on complaints takes place within the framework of the Data Protection Act [1], section 12, subsection. 1 and Article 5 of the Data Protection Regulation [2].

The Data Council has decided to state exceptionally that one of the council members did not believe that the Danish Data Protection Agency was competent to deal with the issue, as the matter is covered by the DA / LO agreement on control measures, which is why the member believed that the trade union system was the right forum.

The Danish Data Protection Agency also finds that [Company B]'s processing of information on complaints is in accordance with Article 32 (1) of the Data Protection Regulation. 1.

Below is a more detailed review of the case and a justification for the Danish Data Protection Agency's decision.

2. Case presentation

It appears from the case file that [Company B] processes complaints information in the form of information about his fingerprints. The processing takes place as part of a control measure that [Company B] has introduced in accordance with the DA / LO agreement on control measures.

[Company B] uses the Biostar V1.92 system, which generates a template of the individual employee's fingerprint, and therefore no images of the fingerprint are processed.

It also appears from the case that there has been an ongoing dialogue between complainants, […], and [Company B] - as well as the parties' professional organizations - about the introduction of the system that registers fingerprints, including in relation to issues of legal authority and security.

2.1. [Trade Union A] ’s remarks

[Trade union A] has stated in the complaint that [the association] on 5 November 2018 received an inquiry from complainants, […]. The inquiry concerned that [Company B] had informed the employees, including complaints, that they had to leave their fingerprints, as the company wanted to introduce a system for registering coming / walking times.

[Trade union A] has further stated that the employees do not know exactly what the system is to be used for in addition to come / go registrations. Employees have been given no justification for why it should be introduced or why their current access

system can no longer be used. Employees are insecure when using this type of registration, as they do not trust that the data security at the company lives up to current rules, as former employees continue to appear in the system and outsiders can use the company's computers.

[…], Complains, has on behalf of the employees approached the management to draw attention to the insecurity and concern of the employees. Complainants have also tried several times to find out what legal basis the processing takes place, how the information is processed and stored with regard to security, and whether the company has had contact with the Danish Data Protection Agency.

The only thing complainants have been told is that [Company B] believes that the company complies with the applicable rules. For complaints, the company has sent documentation from the supplier of the system showing that the system complies with the data protection legislation. However, the company has still not described the purpose of the processing of fingerprint information or referred to a legal basis for the processing.

In [Trade Union A]'s view, it is contrary to the Data Protection Regulation to introduce this type of registration without any legal basis. Furthermore, it is [Fagforening A] 's opinion that the DA / LO agreement on control measures does not provide a legal basis for the processing of biometric information, which is prohibited from processing in accordance with the Data Protection Regulation. According to [Trade Union A], whether the case has been raised under trade union law or not has no significance for the Danish Data Protection Agency's processing of the case.

[Trade union A] also does not believe that the requirement of necessity is met, as the purpose of the treatment can be achieved with less intrusive means. It is not clear why [Company B] believes that food security considerations make it necessary to use employees' fingerprints instead of using a personal tag, card or password. Food safety is important for all food businesses, but [the union] does not agree that the use of fingerprints is the only way to be able to maintain food safety requirements. Other slaughterhouses in the industry - the collective agreement covered by [Trade Union A] - use access control and / or time registration with a personal tag, card or code.

[Trade union A] has also stated that regardless of the standard to which a company is subject, it is the company's responsibility that the procedures laid down by the company for implementing a standard comply with the country's applicable legislation. [Company B] 's certifications therefore do not justify the need, as one can easily comply with the certification by using other and less intrusive means.

[Trade union A] has finally pointed out that at present no fingerprints are used to provide access to the company, but for registration of come / go time and break time. A key tag is used to access the company.

2.2. Dansk Industri's remarks

Dansk Industri has initially stated that the access control has been notified in accordance with the DA / LO agreement on control measures. As the processing of the information is thus based on a collective agreement, its justification should be processed in the trade union legal system, where the Labor Court must ultimately assess whether the processing is justified under the DA / LO agreement on control measures, cf. 1. A case has not been raised by [Trade Union A] in the trade union legal system regarding the justification of the access control.

As the access control is a control measure authorized by the DA / LO agreement on control measures, it is Dansk Industri's opinion that the use of templates of fingerprints for access control is based on the Data Protection Act, section 7, subsection. 2 and § 12, para. 1.

Regarding the operational justification, Dansk Industri has stated that [company B] is a cattle slaughterhouse in […]. The slaughterhouse has a slaughter capacity of […] cattle per week and employs […] staff.

As a slaughterhouse, the company's production is subject to a number of regulatory requirements in accordance with food legislation in relation to production. In addition, the company is affiliated with certification schemes where the slaughterhouse is audited in relation to whether the slaughterhouse meets a number of requirements for quality and safety in production. The slaughterhouse is certified partly by the organization IFS and partly by the organization SAI Global.

It is a general requirement of customers - typically retail customers - that slaughterhouses be affiliated with such certification schemes to ensure the highest possible food safety.

To ensure food safety, one of the elements of the IFS certification is who has access to the production areas. This is to ensure that unauthorized persons do not gain access to the production and to ensure that it can be identified at any time who has participated in the production of a given product, if infection or other irregularities / foreign bodies are subsequently found in a product.

Section 6.2.1 of the IFS standard, version 6.1, provides as follows:

Based on a hazard analysis and assessment of associated risks, identified areas critical to security shall be adequately protected to prevent unauthorized access. Access points shall be controlled ”.

The introduction of the access control in question at [Company B], where fingerprints are used, is precisely intended to ensure food security adequately in accordance with the IFS standard, including in particular to ensure compliance with the above-mentioned point 6.2.1 of the IFS standard. The company has previously used key tags that employees scan, but it is the company's assessment that this solution does not provide sufficient assurance that it can be unambiguously identified who has been present in the production, as there may be theft of key tags or exchange of key tags both erroneously and intentionally.
When exporting to third countries, there are often requirements for separate food certificates in accordance with the legislation of the exporting country, which also presupposes a high level of food security. There is a strong focus on complying with these requirements, as failures in this area could potentially harm export opportunities for the entire industry.
As a consequence, certification according to the IFS standard or equivalent standards is a general customer requirement in the industry, and the use of access control via fingerprints is therefore widespread in the industry and is also used by a number of food companies other than [Company B].
Dansk Industri has further stated that it is [Company B]'s view that the processing of the information is in accordance with the general principles in Article 5 of the Data Protection Regulation, as the general principles largely reflect the same considerations as the assessment under the control measures agreement. based on.
In this connection, Dansk Industri has stated in detail that [Company B] has assessed that the necessary assurance that the company can live up to the safety requirements that follow from the IFS certification and the customers' requirements for this can only be achieved by using fingerprints. at the access control. Given that access control is justified by a consideration for food security, it is the company's assessment that this consideration outweighs the consideration for the individual employee.
In addition, Dansk Industri has stated, including about security, that the system does not store images of the individual fingerprint, but a unique template based on the fingerprint. This template can not be converted back to an image of the employee's fingerprints and can therefore not be used or misused for other purposes for this reason alone. The scanner is designed so that data in the scanner - should the scanner fall into the wrong hands - will not be usable without a copy of the associated database.
The information in the system is stored on a centrally located server. The server is located at the group's head office in […] in a server room that only the IT department's employees have access to via a separate coding system. Outsiders do not have access to the company's PCs, as employees - who have access to PCs as part of their work - have unique logins.

The template associated with the individual employee's fingerprints is deleted when the employee resigns and cannot be subsequently recreated. This is a fixed procedure to ensure that a resigned employee cannot gain access to production. If a former employee is re-employed, the employee must thus be re-created in the system. It is unclear what complaints mean by former employees appearing in the system, as the system was implemented in mid-March 2019.

The Biostar system allows for further encryption of templates and the other information about the employee that is present in the system. Based on the above features, which the company has assessed as attractive, this is not currently implemented.

In relation to the question of notification of the control measure, Dansk Industri has stated that

partly there have been a number of initial discussions with complainants […] and with [Trade Union A]. The notification was formally made at a SU meeting on 30 January 2019.

In connection with this, two meetings were also held in the company's canteen, where the then director answered the employees' questions about the system.

In addition, [Trade Union A] has already been informed in an e-mail of 22 November 2018 that this is an access control - ie a control measure - and that its introduction depends on the requirements set in accordance with the IFS standard.

In connection with the implementation of the access control at [Company B], […] has been in charge of the practical implementation and has in this connection been present at the company on 18 March 2019, when the employees registered the template from their fingerprints in the system.

On this occasion, each employee was talked to and explained about the system and the background to it, just as the employees have had the opportunity to ask questions.

Although [Company B] does not recognize the description in the complaint and does not agree with it, the company will consequently carry out further activities where the employees are informed about the system and its purpose, so that the employees who may feel insecure are taken care of.

In relation to what [Trade Union A] stated in this regard, Danish industry has stated that it is correct that a key tag is used at the company's outer door to unlock the door. Fingerprints are used when the employees enter the production areas, as the purpose as previously described is - for the sake of food safety - to be able to document which employees have participated in the production.

There is no link between the registration of who has participated in the production and the company's working time registration

or payroll system. These are two separate systems that cannot talk to each other, but in the long term [Company B] is considering using the information from the access control to accurately calculate the individual employee's working hours.

Justification for the Danish Data Protection Agency's decision

3.1.

According to Article 2 (1) of the Data Protection Regulation, 1, applies to the processing of personal data carried out in whole or in part by means of automatic data processing, and to other non-automatic processing of personal data which is or will be contained in a register.

It is the Data Inspectorate's opinion that both in connection with the collection (enrollment [3]) of the imprint of a finger, which must form the basis for biometric recognition or identification, and in the subsequent use (matching) of the imprint in connection with the biometric solution , is a processing of personal data covered by the Data Protection Regulation.

The term biometric data is defined in accordance with Article 4 (14) of the Regulation as personal data which, as a result of specific technical processing concerning the physical, physiological or behavioral characteristics of a natural person, enable or confirm an unambiguous identification of the person, e.g. face image or fingerprint information.

The processing of fingerprint information in the form of templates will therefore constitute a processing of biometric data.

Following the wording of Article 9 (1) of the Data Protection Regulation 1, biometric data, including fingerprint information, should only be considered as a special category of information when processing is carried out for the purpose of uniquely identifying a natural person.

In the Data Inspectorate's view, a distinction must therefore be made between whether processing takes place for the purpose of uniquely identifying a natural person, or whether processing takes place for other purposes - e.g. verification (authentication).

This will be a treatment with the aim of uniquely identifying a natural person who is covered by the prohibition in Article 9 (1) of the Regulation. 1, when comparing information about a person's fingerprints (collected at the time of identification) with a series of biometric templates stored in a database so that one or more match processes take place [4].

On the basis of what has been stated in the case, the Danish Data Protection Agency finds that it can be assumed that the solution in question in the case works by matching the employee's fingerprint (template) against a database containing the employees' fingerprints, so that unique identification of which employee is approaching and leaving the workplace. It is

therefore a matter of dealing with specific categories of information covered by the prohibition in Article 9 (1) of the Regulation.

1.

Under Article 88 of the Data Protection Regulation, Member States may, by law or by collective agreement, lay down more specific provisions to ensure the protection of the rights and freedoms of employees' personal data in employment relationships.

The possibility of laying down special national rules pursuant to Article 88 of the Data Protection Regulation is utilized in section 12 (1) of the Data Protection Act. 1, which states that the processing of personal data in connection with employment relationships is covered by Article 6, para. 1, and Article 9, para. 1 may take place if the processing is necessary to comply with the data controller's or data subject's employment law obligations or rights as stipulated in other legislation or collective agreements.

The special comments on the provision state that processing may take place if the processing is necessary to comply with the data controller's or data subject's labor law obligations or rights, as stipulated in other legislation or collective agreements, including the DA / LO agreement on control measures.

A processing of personal data in employment relationships can therefore take place within the framework of the Data Protection Act, section 12. 1, b.a. in cases where the processing takes place as part of a control measure introduced in accordance with the DA / LO agreement on control measures.

As there is agreement in the case that the introduced control measure is covered by the DA / LO agreement on control measures, the Danish Data Protection Agency is of the opinion that the processing takes place within the framework of the Data Protection Act, section 12, subsection. 1.

3.2.

The processing of personal data which takes place in an employment relationship must not, as in the case of all processing, go beyond the basic principles for the processing of data set out in Article 5 of the Data Protection Regulation, including point ac of that provision, on "reasonableness". legitimate purposes ”and“ data minimization ”.

The Danish Data Protection Agency has assumed that the processing currently takes place solely for the purpose of access control, as this has been stated by [Company B]. In this connection, the Danish Data Protection Agency notes that the Authority processes cases on a written basis and on the basis of what is provided by the parties to the case.

The processing of biometric data, including fingerprint data, in the context of access control is not in itself contrary to the fundamental principles of the Data Protection Regulation for the processing of personal data.

[Company B] has stated that it is crucial for food safety, including the company's export opportunities, that unauthorized persons do not gain access to the production, and that it can be identified at any time who has participated in the production of a given product, if subsequently found. infection or other irregularities / foreign bodies in a product. Key tags that employees scan do not provide sufficient assurance that it can be unambiguously identified who has been present in the production, as there may be theft of key tags or replacement of key tags both incorrectly and intentionally.

On the basis of the information available, the Danish Data Protection Agency finds that the purpose - food safety - constitutes a factual operational consideration, just as the Authority finds that there is no basis for overriding [Company B]'s assessment that this purpose necessitates the processing of information about complainants' fingerprints. to eliminate the potential risk that theft of key tags or replacement of key tags may pose. At the same time, considering that [Company B] only processes a template of the fingerprint and not an actual image of the fingerprint, on the present basis, the Danish Data Protection Agency's view is that the processing of information on complaints does not contravene the Data Protection Regulation. Article 5, paragraph 1, letter a-c.

3.3.

It follows from Article 32 (1) of the Data Protection Regulation 1, that taking into account the current technical level, the implementation costs and the nature, scope, coherence and purpose of the processing in question as well as the risks of varying probability and seriousness of natural persons' rights and freedoms, the data controller and data processor implement appropriate technical and organizational measures to ensure level of safety appropriate to these risks.

After reviewing the case, the Danish Data Protection Agency finds that [Company B]'s processing of information on complaints is in accordance with Article 32 (1) of the Data Protection Regulation. 1.

The Danish Data Protection Agency has emphasized that the system does not store images of the individual fingerprint, but a unique template based on the fingerprint, that the scanner is designed so that data in the scanner - should the scanner fall into the wrong hands - will not could be used without a copy of the associated database, that the database that is central to the system is located on a server at the group's head office in a server room that only the IT department's employees have access to via a separate code system, that outsiders do not have access to the company's PCs, as employees - who have access to

PCs as part of their work - have unique logins, and that the information in the system can only be accessed by the few employees who have a work-related need for it, which only includes IT department and the group's payroll office.

3.4.

The Danish Data Protection Agency has also found that in the case there is disagreement about the extent to which the employees, including complaints, have received (sufficient) information about the control measure.

In this connection, the Danish Data Protection Agency notes that the rules of the Data Protection Ordinance and the Data Protection Act on the duty to provide information apply. It is thus a precondition that the employees receive information about the purpose and scope of the processing and about the use of the information collected, in accordance with Article 13 of the Data Protection Regulation. In this connection, reference is made to the guide on the data subjects' rights, which can be found on the Danish Data Protection Agency's website.

The Danish Data Protection Agency has noted that [Company B] in the light of the present complaint will carry out further activities, where the employees are informed about the system and its purpose, so that the employees who may feel insecure are taken care of.

[1] Act No. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).

[3] That is, where the first object is scanned, which is to form the basis for the calculation of the mathematically calculated value - e.g. an image of the full fingerprint. A mathematically calculated value of a biometric imprint is called a template.

[4] This is the process by which biometric information / templates (collected during registration) are compared with the biometric information / templates collected from a new sample for identification, verification / authentication or categorization.