Indicative opinion on the use of fingerprints for the purpose of recording employee arrival / departure times

Date: 29-05-2019

Decision

Private companies

The Danish Data Protection Agency has issued an advisory opinion on the issue of the use of fingerprints (templates) for the purpose of registering employees 'arrival / departure times as part of the control of employees' working hours.

Journal number 2018-211-0135

Summary

The Danish Data Protection Agency has received an inquiry from a lawyer who, on behalf of a client, requested the Authority's position on whether the processing of information on employees' fingerprints (templates) for use in registering employees' arrival / departure times as part of checking employees' working hours can be considered necessary for legal claims to be established, asserted or defended in accordance with Article 9 (1) of the Data Protection Regulation. 2, letter f.

Processing of biometric data - such as fingerprint information - for the purpose of uniquely identifying a natural person, is covered by Article 9 of the Data Protection Regulation on sensitive information in accordance with the Data Protection Regulation.

The Danish Data Protection Agency stated - after the case had been considered by the Data Council - that the ban on processing information about an employee's fingerprints, including templates, in Article 9 (1) of the Regulation. 1, for the purpose of registering the arrival / departure times of employees can not be deviated from with reference to Article 9 (1) of the Data Protection Regulation. 2, letter f (legal requirements) when processing takes place as part of a control of an employee's working hours.

The Danish Data Protection Agency also had occasion to consider whether the processing of employees 'fingerprints in order to check employees' arrival / departure times as part of time control could take place on the basis of a consent from the employee.

In this connection, the Danish Data Protection Agency assessed that an employee's consent for an employer to process information about his or her fingerprints in connection with time control, which the clear starting point cannot be considered to have been given voluntarily and thus constitute a valid basis for processing.

Decision

1.

The Danish Data Protection Agency hereby returns to the case where, on behalf of TimePlan A / S, you have contacted the Authority regarding the use of fingerprints (templates) for use in registering employees 'arrival / departure times as part of checking the employees' working hours.

Processing of biometric data - such as fingerprint information - for the purpose of uniquely identifying a natural person, is covered by Article 9 of the Data Protection Regulation on sensitive information in accordance with the Data Protection Regulation.

The Danish Data Protection Agency's practice regarding the use of fingerprints concerns the previous legal basis in the Personal Data Act, and the case has therefore been submitted to the Data Council.

The Danish Data Protection Agency must then state the following:

The prohibition on the processing of data on an employee's fingerprints, including templates, in Article 9 (1) of the Regulation. 1, for the purpose of recording employee arrival / departure times may not be deviated from with reference to Article 9 (1) of the Data Protection Regulation. 2, letter f (legal requirements) when processing takes place as part of an employee's working hours, as the necessity requirements of the provision are not met.

Below is a presentation of the case and a justification for the Danish Data Protection Agency's opinion.

2. Case presentation

On behalf of TimePlan A / S, you have contacted the Danish Data Protection Agency regarding the use of fingerprint scanning for the purpose of registering employees' arrival / departure times.

You have stated that TimePlan A / S has developed the program, TimePlan, which is used by customers in connection with an efficient and economical solution of shift planning for time registration right up to the preparation of payroll data, which is transferred from the program to customers' payroll systems.

The program is modular, and one of the modules is used for time registration. In this connection, it is possible to connect a fingerprint scanner, so that the program can use fingerprints (templates) to ensure which employee uses the scanner in connection with the employee meeting or leaving the workplace, so that an accurate identification of the person in question takes place. employee.

The customers who use the module in TimePlan only use it to ensure that correct registration of attendance can be made, so that there is a correct basis for calculating salary, salary supplements, etc. For the sake of customers and users of the program, Timeplan A / S would like to ensure that the future use of the function can be considered covered by Article 9 (1) of the Data Protection Regulation. 2, letter f, on the determination of legal claims.

Employee fingerprint information will be stored as templates stored encrypted in a central database.

You have asked the Danish Data Protection Agency to confirm that the described use of templates calculated on the basis of fingerprints can be used as outlined.

3. Legal basis for the Danish Data Protection Agency's opinion

3.1. Scope of the Data Protection Regulation

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.

According to Article 4 (1) of the Regulation, personal data means any information relating to an identified or identifiable natural person ('the data subject').

It is the opinion of the Data Inspectorate that both in connection with the collection (enrollment [1]) 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.

3.2. The category of information

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 information on fingerprints, 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 unambiguously 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, which are stored in a database, so that one or more match processes take place [2].

On the basis of what has been stated in the case, the Danish Data Protection Agency finds that it can be assumed that TimePlan A / S 'solution works by matching the employee's fingerprint (template) against a database containing the employees' fingerprints, so that unambiguous identification of which employee is approaching and leaving the workplace and when this happens. It is therefore a matter of processing specific categories of information covered by the prohibition in Article 9 (1) of the Regulation. 1.

Pursuant to Article 9 (1) of the Data Protection Regulation However, a prohibition applies to the processing of data covered by Article 9 of the Regulation. However, the prohibition does not apply if one of the exceptions in Article 9 (1) of the Data Protection Regulation. 2, or the conditions in the Data Protection Act § 7 are met.

3.3. Processing is necessary for legal claims to be established, asserted or defended

The prohibition in Article 9 (1) of the Data Protection Regulation 1, against the treatment of i.a. biometric data for the purpose of uniquely identifying a natural person finds according to the provision paragraph. 2, letter f, does not apply if processing is necessary for legal claims to be established, asserted or defended, or when courts act in their capacity as a court.

It is the opinion of the Danish Data Protection Agency that an employee's claim for (legal) salary - and the employer's claim to pay only the salary to which the employee is entitled - can be considered to constitute a legal claim.

In the opinion of the Danish Data Protection Agency, the requirement of necessity in Article 9 (1) of the Data Protection Regulation 2, letter f, however, that treatment must be more than just a practical way of fulfilling the purpose, just as the requirement of necessity implies that the purpose must objectively not be reasonably achievable by less intrusive means.

The Danish Data Protection Agency is of the opinion that control of employees' arrival / departure times can be carried out with less intrusive means, which do not necessitate the processing of sensitive information. It will e.g. be able to check when an employee has come and gone from the workplace by using access cards or other similar measures - possibly in combination with other measures, including random checks or manual (personal) checks at the entrance.

The risk of cheating when using other and less intrusive solutions - e.g. access cards or the like - are in the opinion of the Danish Data Protection Agency not of such a nature that this necessitates a systematic processing of biometric information. It is thus the Data Inspectorate's assessment that the possible benefits of a solution such as the present one cannot outweigh that the solution depends on the use of information covered by Article 9.

Against this background, the Danish Data Protection Agency considers that the necessity requirement in Article 9 (1) of the Data Protection Regulation 2, letter f, is not met.

3.4. Consent

The Danish Data Protection Agency has had occasion to consider whether the processing of employees 'fingerprints in order to check employees' arrival / departure times as part of time control could take place on the basis of a consent from the employee.

The prohibition on the processing of sensitive data, including the processing of biometric data for the purpose of uniquely identifying a natural person in Article 9 (1) of the Data Protection Regulation. Paragraph 1 shall not apply if the data subject has expressly consented to the processing of such personal data for one or more specific purposes, unless it is provided by Union law or the national law of the Member States that The prohibition referred to in paragraph 1 may not be lifted with the consent of the data subject, in accordance with Article 9 (1) of the Regulation. 2, letter a.

Article 4 (11) of the Data Protection Regulation states that the consent of the data subject means any voluntary, specific, informed and unambiguous expression of the data subject's consent, whereby the data subject agrees by declaration or clear confirmation that personal data relating to the person concerned is made the subject of treatment.

Article 7 (1) of the Data Protection Regulation 1-4, contains the conditions for consent as a basis for treatment. It follows that:

If processing is based on consent, the data controller must be able to demonstrate that the data subject has given consent to the processing of his personal data.

If the data subject's consent is given in a written statement which also relates to other matters, a request for consent must be submitted in a way that is clearly distinguishable from the other matters, in an easily understandable and easily accessible form and in a clear and simple language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

The data subject has the right to withdraw his consent at any time. Withdrawal of consent does not affect the lawfulness of the

treatment based on consent before the withdrawal. Before consent is given, the data subject must be informed that the consent can be withdrawn. It must be as easy to withdraw his consent as to give it.

When assessing whether consent has been given freely, the greatest possible consideration is given, e.g. on the performance of a contract, including on a service, is made conditional on consent to the processing of personal data which is not necessary for the performance of this contract.

In addition, it follows from the Data Protection Act, section 12, subsection 3, that the processing of personal data in employment may take place on the basis of the data subject's consent in accordance with Article 7 of the Data Protection Regulation.

It is thus a condition for being able to use consent as a basis for treatment that the consent is i.a. voluntarily, which e.g. implies that the employee has a real and free choice and control over the processing of his personal data.

Due to the relationship of dependence between an employer and an employee, in the opinion of the Danish Data Protection Agency, it is doubtful whether an employee can refuse to give an employer his consent to the processing of information about his or her fingerprints in order to check the employee's coming / going times without fear or real risk that the rejection will be detrimental to the person or without feeling some pressure [3].

It is against this background that the Danish Data Protection Agency is of the opinion that an employee's consent for an employer to process information about his or her fingerprints in connection with time control, which the clear starting point cannot be considered to have been given voluntarily. If a consent can not be considered voluntary, it can not constitute a valid basis for treatment. However, the Danish Data Protection Agency cannot deny that there may be special circumstances under which consent can be considered voluntary.

[1] 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.

[2] 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.

[3] In this context, reference is made to page 7 of the Article 29 Working Party Guidelines on Consent under the Data Protection Regulation (WP259) and the Consent Guidelines available on the Authority's website.