The Danish Data Protection Authority has made a decision in a case about the use of a system for facial recognition

Date: 17-03-2022

Decision

Private companies

Warning

Supervision / self-management case

Biometrics

Sensitive information

Basis of treatment

The Danish Data Protection Authority has made a decision in a case which concerned the processing of information about biometric data using a facial recognition system. The purpose of the treatment was, among other things, to control access to the company's facilities.

Journal Number: 2021-431-0145

Summary

In a case that the Danish Data Protection Authority started on its own initiative, the Danish Data Protection Authority has dealt with FysioDanmark Hillerød ApS' intended use of a facial recognition system, which was to be used, among other things. to conduct access control with customers and employees.

Based on the circumstances of the case and the information provided by the company, the Danish Data Protection Authority assessed that the system – which was based on the data subject's consent – could be used within the framework of the data protection rules.

However, the Norwegian Data Protection Authority found reason to warn the company that it would probably be in breach of the rules in the data protection regulation if the company used the system without the consent of the company's customers.

Furthermore, the Danish Data Protection Authority warned that it would probably be in breach of the rules of the data protection regulation if the company did not ensure that the system was not used in relation to persons who had not given their consent.

1. Decision

The Danish Data Protection Authority hereby returns to the case where, on 7 July 2021, the Danish Data Protection Authority chose on its own initiative to investigate FysioDanmark Hillerød ApS' (hereafter FysioDanmark) processing of personal data using a facial recognition system.

In the decision, the Danish Data Protection Authority has only dealt with whether Article 6 and Article 9 of the Data Protection Regulation can form a basis for processing personal data, and the Danish Data Protection Authority has thus not taken a position on any other data protection law issues.

The Danish Data Protection Authority issues a warning to FysioDanmark that it is likely to be in breach of the data protection regulation[1] if FysioDanmark:

for the use of statistics and business optimization, processes biometric data with the aim of uniquely identifying a registered person, without obtaining consent from the person concerned in accordance with the data protection regulation, article 9, subsection 2, letter a.

uses the facial recognition system in the planned manner, as this will involve processing of biometric data with the aim of uniquely identifying a natural person about the persons who did not wish to consent to the processing, which is prohibited, as no exception to this can be identified in the regulation's article 9, subsection 2.

The warning is given in accordance with the data protection regulation's article 58, subsection 2, letter a.

Below follows a closer review of the case and a rationale for the Data Protection Authority's decision.

2. Information provided by FysioDanmark for use in the case

2.1.

FysioDanmark has stated that on 24 September 2020, FysioDanmark has entered into a collaboration with the company Justface ApS, which has delivered a system based on facial recognition (the "system").

The system has not yet been put into use.

The system works in such a way that a camera is set up at the entrance to the fitness centre, which can scan the faces of customers and employees, after which the result is compared to images already uploaded in the system.

Once the system is put into use, the system is "online" continuously.

FysioDanmark is the data controller for the processing of personal data that takes place, and Justface ApS is the data processor.

The purpose of using the system - and the resulting processing of personal data - is, firstly, to offer customers and employees to use the system as access control rather than access control with a physical access card and password.

The processing of biometric information (face recognition) in connection with access control is based on the customer's / employee's consent. It is thus voluntary whether customers and employees wish to use the system as access control.

Consent is given when the customer / employee is to be created in the system - either physically in the center or online. In this connection, a picture of the person's face is uploaded to the system. In addition, the person in question consents via an electronic consent form that the processing may take place. The declaration of consent has the following wording:

"Declaration of consent

By checking the consent boxes below, I give my consent for FysioDanmark Hillerød, Milnersvej 39, 3400 Hillerød, to process the following personal data about me for the purposes described below. FysioDanmark Hillerød encourages that the declaration of consent be read thoroughly before consent is given.

I hereby consent to FysioDanmark Hillerød processing my personal data for the following purposes:

Which categories of personal data are processed?

General personal information (we only request this information if it is not already filled in with your gym)

Name

Date of birth

Address

E-mail

Portrait image

Confidential and sensitive personal data

Biometric information in the form of a face scan

For what purposes is your personal data processed?

Your personal data is processed for the purpose of checking the validity of your membership when accessing the fitness centre.

How is your personal data collected?

We collect your personal data from your user profile at the fitness center and from yourself in such a way that you will be asked

to update your information via your user profile in our app or website. This is to ensure that the gym always has the correct information on their members.

Biometric scanning takes place at the entrance to the fitness centre. The scan is used to compare your picture with the profile picture you have uploaded to your user profile at the gym, so that we can validate your membership at the gym.

How is your personal data processed?

Processing of personal data takes place pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data ("GDPR") and the Danish data protection law.

Your personal data will be passed on to the fitness center you use, as well as to the fitness center's (data) administration company - this can be FlexyBox ApS, Sport Solution A/S or Globus Data ApS. These are in each case responsible for the processing of your data in their own systems. We therefore also refer to the fitness center's and management companies' respective personal data policies for further information on their processing of personal data.

Your personal data is processed by Justface according to the purposes described above, and only to the extent that it is strictly necessary.

Your personal data will only be accessible to relevant and specially designated persons at Justface, and will only be passed on to others if required according to the described purposes or if required by law.

Further information about Justface's privacy policy can be found on our website: www.justface.dk

[…]

Withdrawal of consent

Giving consent is voluntary and you are entitled to withdraw your consent at any time. If you wish to revoke your consent, simply contact Support@justface.dk, who will then contact the fitness center and the management company to register that your consent has been revoked.

If you do not wish to give consent, or if you revoke your consent, it is not possible to use a biometric scan and we therefore ask you to contact your fitness center to hear about alternative solutions.

[…]”

Consent is obtained in FysioDanmark's opinion in accordance with the data protection regulation's conditions for a (valid)

consent, in that:

it is voluntary for the customer/employee whether the person concerned will give consent or not, which is expressly stated in the declaration of consent,

it is stated on the declaration of consent that a consent can be revoked at any time,

the data subjects receive information about what the purposes of the consent are, and the data subjects must tick separate consent boxes in relation to the respective purposes, and

a link has been inserted in the consent text to further information on how FysioDanmark processes information about customers and employees respectively.

If a customer or employee does not wish to use the system, a physical access card and password can be used instead. If this is the case, no facial recognition of the person in question takes place, as the system must use a stored image to perform the facial recognition.

In these cases, the use of the system can therefore rather be equated with ordinary TV surveillance - albeit with the differences that the images from the surveillance are not stored in the system's memory, and that the images from the system cannot be accessed and/or monitored by the gym's staff (or by Justface). .

Any processing of personal data carried out in relation to persons who have not given consent is not covered by Article 9 of the Data Protection Regulation. Such processing will therefore be carried out on the basis of e.g. the data protection regulation, article 6, subsection 1, letter f.

2.2.

In addition to access control, the system is used to collect and process information about FysioDanmark's customers for statistics and business optimization, including optimization of staff allocation in relation to the fitness center's peak load periods.

Information about the length of time the customer is in the gym is collected by the system registering when a customer enters the gym door and when the customer leaves the gym door. The information is therefore only collected if the customer has given consent to use the system.

This information, which is only collected for statistical purposes and for business optimization, is not covered by Article 9 of the Data Protection Regulation.

The information in question can be collected and processed on the basis of Article 6, paragraph 1 of the Data Protection Regulation. 1, letter f.

The information is not collected about the employees.

3. The Data Protection Authority's reasoning

3.1. Relevant legal regulations

The Data Protection Regulation finds, according to Article 2, paragraph 1, application to processing of personal data that is carried out in whole or in part by means of automatic data processing, and to other non-automatic processing of personal data that is or will be contained in a register.

Of the data protection regulation, article 6, subsection 1, it appears that processing is only lawful if and to the extent that at least one of the following conditions applies:

The data subject has given consent to the processing of his personal data for one or more specific purposes.

Processing is necessary for the performance of a contract to which the data subject is a party, or for the implementation of measures taken at the data subject's request prior to entering into a contract.

Processing is necessary to comply with a legal obligation owed to the data controller.

Processing is necessary to protect the vital interests of the data subject or another natural person.

Processing is necessary for the performance of a task in the interest of society or which falls under the exercise of public authority, which the data controller has been tasked with.

Processing is necessary for the controller or a third party to pursue a legitimate interest, unless the data subject's interests or fundamental rights and freedoms requiring the protection of personal data take precedence, in particular if the data subject is a child.

According to the data protection regulation's article 9, subsection 1, a prohibition applies to the processing of special categories of information, including the processing of biometric data for the purpose of uniquely identifying a natural person.

According to Article 4, No. 14 of the Data Protection Regulation, biometric data means personal data which, as a result of specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, enables or confirms a unique identification of the person concerned, e.g. facial image or fingerprint information.

The prohibition in the data protection regulation article 9 paragraph 1, finds according to the provision subsection 2, does not

apply if one of the following conditions applies:

The data subject has given express consent to the processing of such personal data for one or more specific purposes, unless it is stipulated in EU law or the national law of the Member States that in subsection The prohibition referred to in 1 cannot be lifted with the data subject's consent.

Processing is necessary to comply with the labor, health and social law obligations and specific rights of the data controller or the data subject, insofar as it is based on EU law or the national law of the Member States or a collective agreement pursuant to the national law of the Member States which provides necessary guarantees for the data subject's fundamental rights and interests.

Processing is necessary to protect the vital interests of the data subject or another natural person in cases where the data subject is physically or legally unable to give consent.

Processing is carried out by a foundation, an association or another body which does not work for profit and whose aim is of a political, philosophical, religious or trade union nature, as part of the body's legitimate activities and with the necessary guarantees, and on condition that the processing only concerns the body's members, former members or persons who, due to the body's purpose, are in regular contact with it, and that the personal data is not passed on outside the body without the data subject's consent.

Processing concerns personal data that is clearly published by the data subject.

Processing is necessary for legal claims to be established, asserted or defended, or when courts act in their judicial capacity.

g) Processing is necessary for reasons of significant public interest on the basis of EU law or the national law of the Member States and is proportionate to the objective pursued, respects the essential content of the right to data protection and ensures appropriate and specific measures to protect the data subject's fundamental rights and interests.

Treatment is necessary for the purposes of preventive medicine or occupational medicine for the assessment of the worker's occupational capacity, medical diagnosis, the provision of social and health care or treatment or the management of social and health care and services on the basis of EU law or the national law of the Member States or in pursuant to a contract with a healthcare professional and subject to the conditions and guarantees referred to in subsection 3.

Treatment is necessary for reasons of public interest in the field of public health, e.g. protection against serious cross-border health risks or ensuring high quality and safety standards for healthcare and medicinal products or medical devices on the

basis of EU law or the national law of the Member States, which lays down appropriate and specific measures to protect the data subject's rights and freedoms, in particular confidentiality.

Processing is necessary for archival purposes in the interest of society, for scientific or historical research purposes or for statistical purposes in accordance with Article 89, subsection 1, on the basis of EU law or the national law of the Member States and is proportionate to the objective pursued, respects the essential content of the right to data protection and ensures appropriate and specific measures to protect the fundamental rights and interests of the data subject.

With a consent as referred to in the data protection regulation, article 6, subsection 1, letter a, and Article 9, subsection 2, letter a, according to Article 4, no. 11, is understood as any voluntary, specific, informed and unequivocal declaration of intent by the data subject, whereby the data subject, by declaration or clear confirmation, consents to personal data relating to the person concerned being made the subject of treatment.

Article 7 of the Data Protection Regulation contains a number of conditions for consent. It appears from this:

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 that 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 clear and simple language. Any part of such declaration which constitutes a breach 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 processing based on consent prior to the withdrawal. Before consent is given, the data subject must be informed that consent can be withdrawn. It should be as easy to withdraw consent as it is to give it.

When assessing whether consent has been freely given, the greatest possible consideration is given to, among other things on the fulfillment of a contract, including on a service, is made conditional on consent to the processing of personal data that is not necessary for the fulfillment of this contract.

This follows from Section 12, subsection 1 of the Data Protection Act. 3, that processing of personal data in employment can take place on the basis of the data subject's consent in accordance with Article 7 of the Data Protection Regulation

3.2. Processing of personal data about customers who wish to make use of facial recognition

3.2.1. Processing for the use of access control

When personal data is processed in the form of images in connection with face scanning, biometric data is processed, cf. Article 4, No. 14 of the Data Protection Regulation.

FysioDanmark has stated that the system works in such a way that a camera is set up at the entrance to the Fitness Centre, which can scan the customer's face, after which the result is compared to images already uploaded in the system. Biometric information about the customer in question (collected at the time of identification) is thus compared with a number of biometric templates stored in a database.

Thus, one or more match processes take place, and it is therefore a matter of processing biometric data with the aim of uniquely identifying a natural person.

It is basically prohibited to process such information, cf. the data protection regulation's article 9, subsection 1, unless an exception to this prohibition can be identified in subsection (1) of the provision. 2.

In this connection, the Danish Data Protection Authority agrees with FysioDanmark that the customer's express consent, cf. the data protection regulation's article 9, subsection 2, letter a, is the most appropriate exception to the ban, as none of the other exceptions in the data protection regulation, article 9, paragraph 2, is seen to be applicable.

The Danish Data Protection Authority assumes that when using the customer's express consent, FysioDanmark will observe the obligations according to Article 7 of the regulation, and as a result, the Danish Data Protection Authority finds no basis for overriding FysioDanmark's assessment that the consent given by the data subject in that connection complies with to the rules for consent in the data protection regulation, including the requirement that consent must be voluntary in the regulation's article 4, no. 11.

The Danish Data Protection Authority has thereby emphasized the design and content of the submitted declaration of consent, and that it is optional for the customer whether they wish to use facial recognition as access control, as the customer – if they do not wish to use facial recognition – can instead use an access card and code.

3.2.2. Processing for business optimization

It is hereby stated that FysioDanmark – in addition to processing biometric data in connection with access control – collects information via the system for use in statistics, including information on the amount of time customers are in the gym.

In this connection, the Danish Data Protection Authority agrees with FysioDanmark that the information about the time a

customer is in the fitness center is in itself information that is only covered by Article 6 of the Data Protection Regulation. However, the Danish Data Protection Authority is of the opinion that this information is of the nature of "derived" information, as the information is provided through the use of facial recognition.

Information about the period of time is thus collected by the facial recognition system registering when a customer enters the door of the gym and when the customer leaves the gym again.

This is therefore the processing of biometric data for the purpose of unambiguously identifying a natural person covered by the prohibition in Article 9, paragraph 1 of the Data Protection Regulation. 1.

As is the case in relation to access control, it is the Danish Data Protection Authority's assessment that the only possible exception to the prohibition in the Data Protection Regulation, Article 9, subsection 1, the data subject's consent is in accordance with the data protection regulation's article 9, subsection 2, letter a, as none of the other exceptions in the provision appear to apply.

On this basis, the Danish Data Protection Authority must notify FysioDanmark of a warning that it is likely to be in breach of the data protection regulation if FysioDanmark, for the purposes of statistics and business optimization, processes biometric data with the aim of uniquely identifying a data subject without obtaining consent from the person concerned in according to the data protection regulation, article 9, subsection 2, letter a.

The warning is given in accordance with the data protection regulation's article 58, subsection 2, letter a.

If FysioDanmark intends to adapt to the above, the customer's consent will have to be obtained for the processing of biometric data about him in connection with conducting access control with customers and keeping statistics on how long customers stay in the fitness center.

In this connection, the Danish Data Protection Authority can state for information purposes that a consent is not assumed to have been given voluntarily if the procedure for obtaining consent does not give the data subject the opportunity to give separate consent to various processing activities relating to personal data, and is thus forced to consent for all purposes . The consent must therefore be granulated (divided).

If a processing of information serves several purposes, the data controller must thus obtain separate consent for each individual purpose, which must be processed on the basis of the data subject's consent. The data controller must therefore offer the data subject the opportunity to consent for one purpose, but refrain from consenting for other purposes.

In practical terms, this can happen e.g. in the form of an overall statement, where the data subject can mark the purposes for which he/she will accept that information is processed.

3.3. Processing of personal data about employees who wish to use facial recognition

FysioDanmark has informed the case that employees are also offered the use of facial recognition as access control, and that this is used if the employee agrees to this.

For the reasons stated in section 3.2.1, in relation to employees, it is also a matter of processing information about biometric data with the aim of uniquely identifying a natural person, which is basically prohibited to process, cf. the data protection regulation, article 9, subsection 1, unless an exception to this prohibition can be identified in subsection (1) of the provision. 2.

In this connection, the Data Protection Authority agrees with FysioDanmark that the employee's express consent, cf. the data protection regulation's article 9, subsection 2, letter a, is the most appropriate exception to the ban, as none of the other exceptions in the data protection regulation, article 9, paragraph 2, is seen to be applicable.

However, this is only a matter of consent in the sense of the data protection regulation, which can form the basis for processing personal data if the consent is voluntary. The assessment of whether a consent is voluntary includes, among other things, whether there is an unequal relationship between the data controller and the data subject. A consent is normally not considered to have been given voluntarily if there is a clear bias between the data subject and the data controller.

In employment relationships, there is typically an inequality between the employer and the employee.

In this connection, the Danish Data Protection Authority has previously stated that an employee consents to an employer processing information about the person's fingerprints in connection with time control, i.e. for use in checking employees' arrival/departure times, which the clear starting point cannot be considered to have been given voluntarily, unless there are special circumstances.

It thus depends on a concrete assessment of whether the employee can voluntarily give consent, which can form the basis for processing information about the person concerned.

FysioDanmark has stated that – as is the case for customers – it is also voluntary in relation to employees, whether the person concerned wishes to use facial recognition in connection with access to the fitness centre. If an employee does not wish to use the system, the person in question can instead use a physical access card and password.

The Danish Data Protection Authority also assumes, on the basis of the information in the case, that the system only records

information about the employee in connection with the person's access to the centre. Information about the employee's movement in the center in general is therefore not recorded, including when the person leaves the workplace, which is why the information is not seen to be suitable for use in time recording.

Under these circumstances, the Data Protection Authority does not find sufficient grounds to override FysioDanmark's assessment that the employee's express consent, cf. the data protection regulation's article 9, subsection 2, letter a, cf. section 12, subsection of the Data Protection Act. 3, can be used as an exception to the prohibition in Article 9, subsection 1.

3.4. Processing of personal data about persons, including customers and employees, who do not wish to use facial recognition

FysioDanmark has stated that the camera, which is set up at FysioDanmark's entrance, is "online" continuously.

On this basis, the Danish Data Protection Authority assumes that the camera - and the facial recognition technology stored in it - is thus also active and used in relation to persons who have not consented to the processing in question when they move within the camera's field of view. The system therefore does not have to be "activated" first - e.g. by using keystrokes or the like.

In this connection, FysioDanmark has stated that if a person does not want to make use of facial recognition, no facial recognition of the person in question takes place, as the system must use a stored image to perform the facial recognition. In these cases, the use of the system can therefore rather be equated with ordinary TV surveillance - albeit with the differences that the images from the surveillance are not stored in the system's memory, and that the images from the system cannot be accessed and/or monitored by the gym's staff (or by Justface). .

In FysioDanmark's view, the possible processing of personal data carried out on persons who have not consented to the use of facial recognition is therefore not covered by Article 9 of the Data Protection Regulation.

However, it is the Danish Data Protection Authority's assessment that biometric data will also be processed for the purpose of unambiguous identification of persons who have not consented to the processing.

This is because, according to the wording of Article 9, subsection 1, it is the purpose of the processing itself – for the purpose of unambiguous identification of the data subject through the use of biometric data – that determines whether the processing is covered by Article 9 of the regulation. It is thus irrelevant whether a match occurs, i.e. whether a unique identification actually takes place.

This is also the case, even if the treatment is quite fleeting (short-term).

In this connection, the Danish Data Protection Authority also refers to the EDPB's guidance 3/2019[2], of which the following includes appears:

"A controller manages access to his building using a facial recognition method. People can only use this way of access if they have given their explicitly informed consent (according to Article 9 (2) (a)) beforehand. However, in order to ensure that no one who has not previously given his or her consent is captured, the facial recognition method should be triggered by the data subject himself, for instance by pushing a button. To ensure the lawfulness of the processing, the controller must always offer an alternative way to access the building, without biometric processing, such as badges or keys."

As the facial recognition technology is used continuously, and since biometric data is thus processed with the aim of uniquely identifying the person in question for all registered persons who are caught by the camera's field of view, the use of the facial recognition technology requires the express consent of the registered person(s), cf. Article 9 of the Data Protection Regulation, PCS. 2, letter a, as none of the other exceptions apply.

However, this is not possible, since in relation to this group of registered persons, we are talking about persons who did not want to give consent.

Against this background, the Danish Data Protection Authority issues a warning to FysioDanmark that it will probably be in breach of the data protection regulation if FysioDanmark uses the face recognition system in the planned way, as biometric data will be processed with the aim of uniquely identifying a natural person about the persons , who did not wish to consent to the processing, which is prohibited, as no exception to this can be identified in the regulation's article 9, subsection 2.

The warning is given in accordance with the data protection regulation's article 58, subsection 2, letter a.

It is up to FysioDanmark to respond to the warning, but the Danish Data Protection Authority can advise FysioDanmark to consider setting up the solution in such a way that the system is only "activated" when the customer or employee who wishes to have a facial scan performed , have activated the system – e.g. by pressing a key.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free exchange of such data and on the repeal of Directive 95/46/EC (general regulation on data protection).

[2] EDPB's guidelines 3/2019 on processing of personal data through video devices, version 2.0, 29 January 2020, section 5.1., General considerations when processing biometric data.