DATATILSYNET

9 June 2023

Brøndby IF has been granted permission for the extended use of facial recognition

Following a request from Brøndby IF – and after the matter had been referred to the Data Council – the Danish Data Protection Agency has granted Brøndby IF permission to use (mobile) facial recognition at matches in stadiums other than Brøndby Stadium. Furthermore, Brøndby IF may use images from surveillance cameras at the stadium to register individuals who breach the rules of conduct in the automatic facial recognition system.

Summary

On 24 May 2019, the Danish Data Protection Agency granted authorisation for the processing of special categories of personal data (biometric data for the purpose of uniquely identifying a natural person) in connection with Brøndby IF's implementation of automatic facial recognition as part of access control at the entrances to Brøndby Stadium.

Brøndby IF has subsequently requested permission to also use automated facial recognition at matches in other stadiums. Furthermore, Brøndby IF has requested permission to use images from surveillance cameras at the stadium as a basis for registering individuals who breach the rules of conduct in the automated facial recognition system.

It is the Danish Data Protection Agency's view that the circumstances which led the Agency to grant authorisation for the use of automatic facial recognition as part of access control at the entrances to Brøndby Stadium back in May 2019 must also be considered to apply in relation to Brøndby IF's away matches.

Taking into account that there will be no processing – or only very limited processing – of special categories of personal data (biometric data) concerning others, such as the home team's supporters, the Danish Data Protection Agency has assessed that Brøndby IF may also use (mobile) facial recognition at matches in stadiums other than Brøndby Stadium.

The Danish Data Protection Agency also assessed that Brøndby IF may use images from surveillance cameras at the stadium as a basis for registering individuals who breach the rules of conduct in the automatic facial recognition system.

For the sake of good order, the Danish Data Protection Agency drew Brøndby IF's attention to the fact that the use of images from the surveillance cameras may be subject to the provisions of section 4c(4) and (5) of the CCTV Surveillance Act.

Authorisation

1. On 30 November 2022, DLA Piper Denmark Advokatpartnerselskab, on behalf of Brøndby IF, submitted a renewed application to the Danish Data Protection Agency regarding the extended use of automatic facial recognition.

On 24 May 2019, the Danish Data Protection Agency granted authorisation – pursuant to Section 7(4) of the Data Protection Act – for the processing of sensitive personal data covered by Article 9 of the General Data Protection Regulation – biometric data for the purpose of uniquely identifying a natural person – in connection with the implementation of automated facial recognition as part of access control at the entrances to Brøndby Stadium.

2. Brøndby IF's request

2.1. In the letter dated 30 November 2022, a request is made for Brøndby IF to be permitted to use automated facial recognition at matches held at stadiums other than Brøndby Stadium.

As background to this, the letter states that experience with the use of automatic facial recognition has generally been positive.

However, Brøndby IF has noted that individuals who, under the rules and regulations of Brøndby Stadium, have been banned from attending football matches involving Brøndby IF – regardless of where these matches are played – have managed to gain access to matches at other stadiums, where they have exhibited behaviour similar to that which led to them being banned from attending matches involving Brøndby IF, including acts of violence and vandalism, as well as other behaviour that creates a sense of insecurity – both inside the stadium, in the area surrounding the stadium, and whilst travelling to and from the stadium.

The use of the system will – due to the seating arrangements for supporters at away matches and the procedures for purchasing tickets, etc. – apply solely to individuals identified as supporters of Brøndby IF who are subject to similar processing in connection with matches at Brøndby Stadium.

2.2. A request is also made for Brøndby IF to be permitted to extend the use of automated facial recognition at Brøndby Stadium.

As background to this, the enquiry states that the original application, on which the Danish Data Protection Agency's authorisation of 24 May 2019 was based, was motivated by a desire to be able to refuse entry to individuals who had already been banned from Brøndby Stadium.

However, it can be difficult to apprehend individuals who, whilst lawfully admitted to the stadium, breach the Brøndby Stadium regulations or the Superliga's regulations in such a way that they must be banned – often because it is deemed unsafe for security reasons for stewards to attempt to apprehend the individuals in question during the match, as this may pose a danger or cause significant disruption to other spectators in the area.

Brøndby IF therefore wishes to be able to use images from surveillance cameras at the stadium as a basis for registering individuals who breach the rules of conduct in the automatic facial recognition system, so that the individuals in question can be apprehended when they subsequently attempt to gain access to Brøndby Stadium again.

3. The Danish Data Protection Agency's assessment

The case was considered at a meeting of the Data Council

3.1. It is the Danish Data Protection Agency's view that the circumstances which led the Agency to grant authorisation for the processing in question in connection with the use of automatic facial recognition as part of access control at the entrances to Brøndby Stadium must also be considered to apply in relation to Brøndby IF's away matches, i.e. matches at stadiums other than Brøndby Stadium.

When it is also taken into account that there will be no – or only very limited – processing of special categories of personal data – biometric data for the purpose of uniquely identifying a natural person – concerning others, such as the home team's supporters, it is the Danish Data Protection Agency's assessment that Brøndby IF – within the framework of the authorisation granted on 24 May 2019 – may also use (mobile) facial recognition at matches at stadiums other than Brøndby Stadium.

In this connection, Brøndby IF must pay attention to the physical security of the mobile automatic facial recognition system so that unauthorised persons cannot gain access to personal data in the system.

3.2. Furthermore, it is the Danish Data Protection Agency's assessment that Brøndby IF – within the framework of the authorisation granted – may use images from surveillance cameras at the stadium as a basis for the automatic facial recognition system to register individuals who breach the rules of conduct.

However, Brøndby IF remains obliged to comply with the terms of the authorisation.

This means, amongst other things, that the imposition of a ban – including the use of images from stadium CCTV cameras – must be carried out on an objective and proportionate basis in relation to breaches of the rules of conduct of Brøndby IF and the Superliga.

Furthermore, this means that Brøndby IF must comply with the duty to provide information when collecting personal data. Brøndby IF must also, by means of signage or in some other clear manner, provide information that access control is being carried out, including the processing of biometric data through the use of an automated facial recognition system.

Furthermore, for the sake of good order, the Danish Data Protection Agency must draw Brøndby IF's attention to the fact that the use of images from the surveillance cameras may be subject to the provisions of section 4c(4) and (5) of the CCTV Surveillance Act. This will be the case if the CCTV cameras at the stadium are installed for the purpose of crime prevention, and if Brøndby IF – rather than a template – uses, including in the automated facial recognition system, an actual image derived from the CCTV cameras at the stadium.

If this is the case, Brøndby IF must take note of the following.

It follows from section 4c(4) of the CCTV Act that recordings as referred to in subsection (1), i.e. image and sound recordings containing personal data recorded in connection with CCTV surveillance for the purpose of crime prevention, must be deleted no later than 30 days after the recordings were made, subject, however, to paragraph 5.

The term 'image and audio recordings' covers both still images and moving images.

In the opinion of the Danish Data Protection Agency, this implies that the images from the surveillance cameras at the stadium, which are intended to be recorded in the automatic facial recognition system, must, as a general rule, be deleted no later than 30 days after the recordings are made. This also applies to images that have been 'transferred' to the facial recognition system.

However, it follows from section 4c(5) of the CCTV Surveillance Act that recordings may be retained for a longer period than that specified in subsection (4) if this is necessary for the controller's handling of a specific dispute. If retention is necessary in connection with a specific dispute, the controller must, within the time limit specified in paragraph 4, notify the person to whom the dispute relates and, upon request, provide that person with a copy of the recording.

In the opinion of the Danish Data Protection Agency, it is reasonable to regard Brøndby IF's notification and enforcement of a ban as the handling of a specific dispute. Footage – derived from the stadium's CCTV cameras – may therefore be retained for longer than 30 days.

It is therefore the Danish Data Protection Agency's assessment that section 4c(4) of the CCTV Surveillance Act will not prevent Brøndby IF from using images from surveillance cameras at the stadium as a basis for registering, via the automatic facial recognition system, individuals who breach the rules of conduct.

Unlike the duty to provide information under Article 14 of the General Data Protection Regulation, the duty to notify set out in section 4c(5), second sentence, of the CCTV Surveillance Act is not deemed to contain any exceptions.

Individuals appearing in an image captured by the stadium's CCTV cameras, which is retained for longer than 30 days, will therefore have to be notified of this and will be able to request a copy of the image.