Unauthorized access to video surveillance

Date: 18-06-2020

Decision

Private companies

In connection with a serious security breach, the Danish Data Protection Agency has found that Salling had taken appropriate technical and organizational measures, but criticizes the fact that Salling only reported the incident to the audit 10 days after the company became aware of the episode.

Journal number: 2020-441-4652

Summary

The Danish Data Protection Agency has made a decision in a case where an employee at Salling locked a former employee in the staff entrance and in a closed concierge room and showed the former employee video surveillance material from the business area, which showed pictures of the former employee's ex-boyfriend who was out shopping with a friend.

Despite the episode, the Danish Data Protection Agency found that Salling had taken appropriate organizational and technical measures to ensure a level of security that matched the risks involved in the processing of personal data in question, and that the company could not be held responsible for the incident in question.

In addition to many of the measures Salling has taken, the Danish Data Protection Agency emphasized that an employee knowingly and against better knowledge in several ways, for example by giving a former employee access to the building, broke the company's guidelines. The Danish Data Protection Agency further found that the employee took up to several actions that went beyond what could reasonably be expected that Salling should have been prepared for or taken measures to avoid.

The Danish Data Protection Agency has therefore only expressed criticism of the late notification of the incident to the Authority.

Decision

The Danish Data Protection Agency hereby returns to the case where Salling Group A / S (hereinafter Salling) on 18 January 2020 reported a breach of personal data security to the Danish Data Protection Agency. The review has the following reference number:

a61a346882d03d0c952d254b5d078161ce6409e6

Decision

After a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing criticism that Salling's processing of personal data has not taken place in accordance with the Data Protection Regulation [1], Article 33 (1). 1.

In addition, the Danish Data Protection Agency finds that Salling's processing of personal data has taken place in accordance with Article 32 (1) of the Data Protection Ordinance. 1 and 34, para. 1.

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

2. Case presentation

On 18 January 2020, Salling reported a breach of personal data security to the Danish Data Protection Agency.

It appears from the case that Salling on 8 January 2020 found that an employee guard on 20 December 2019 closed a former employee guard in through the staff entrance and into a closed concierge room, and then gave the former employee access to watch and record video of video surveillance material from the business area on TV screens, which can only be seen in the concierge room. The video showed pictures of the former employee's ex-girlfriend, who was out shopping with a friend.

The former employee then sent the video sequence to the ex-girlfriend, which appeared on the footage. On January 8, 2020, the ex-girlfriend alerted Salling to the incident.

Salling has stated that both the sender and the recipient of the recordings have confirmed that they have deleted the information.

Salling has also stated that access control has been established at the staff entrance. In addition, there is a physical guard in the room to ensure that no unauthorized person has access to the room and the video surveillance. The door to the separate concierge room is locked when no guard is present. Only trusted employees have access to the concierge room. In addition, the video material can only be accessed at Salling Group's headquarters, where only similarly trusted employees have access.

Salling has developed an information security policy, which is available on Salling Group's intranet. The information security policy is revised every two years. The current version is from 2018 and will be revised in 2020. In addition, a version has been prepared for use by employees, which is also available on the intranet.

Salling has further stated that of the company's employment contracts and employee handbook, among other things. states

that information and information that the employee becomes aware of during the employment relationship must be treated confidentially and thus may not be passed on to persons outside the company.

Salling has also stated that in connection with the beginning of the employment, all new employees must undergo two e-learning courses regarding IT security and data protection. In addition, clear, visible signage has been erected on screens showing video surveillance material. Furthermore, in September 2019, an email was sent to all caretakers and parking guards associated with the business, referring to the fact that only material from TV surveillance may be passed on to the police and thus not to other parties. This email was reviewed at an office meeting with porters in the store also in September 2019. In addition, Salling Group can state that the mentioned data security breach has also resulted in the store asking all porters and parking guards to confirm in writing that they have read the applicable rules.

In addition, Salling has stated that one of the two persons concerned brought Salling to the attention of the incident on 8 January 2020. Salling then took the case under consideration for a further clarification of the facts, and on 18 January 2020 made a report of the incident. as a breach of personal data security to the Danish Data Protection Agency.

In conclusion, Salling stated that the company did not inform the two persons appearing in the recordings in accordance with Article 34 (1) of the Data Protection Regulation. In so far as the two persons are concerned, Salling has emphasized that it was one person who brought the incident to the attention of the company and that there is no high risk of the other person's loss of rights or freedoms. Salling also considers it very likely that the person in question has already been informed of the incident by the former person.

Justification for the Danish Data Protection Agency's decision

3.1. Article 32 of the Data Protection Regulation

It follows from Article 32 (1) of the Data Protection Regulation 1, that the data controller must take appropriate technical and organizational measures to ensure a level of security that is appropriate to the risks involved in the data controller's processing of personal data.

On the basis of what Salling stated, the Danish Data Protection Agency assumes that information from Salling's surveillance camera has been passed on to a former employee and his ex-girlfriend.

On this basis, the Danish Data Protection Agency assumes that there has been an unauthorized transfer of personal data to unauthorized persons, which is why the Authority finds that there has been a breach of personal data security, cf. Article 4, no.

12 of the Data Protection Regulation.

However, the Danish Data Protection Agency finds that Salling has taken appropriate organizational and technical measures to ensure a level of security that is appropriate to the risks involved in the processing of personal data in question, cf. Article 32 (1) of the Data Protection Regulation. 1.

In this connection, the Danish Data Protection Agency has emphasized that all Salling's employees must undergo two courses regarding IT security and data protection, that the company has set up clear, visible, signage on screens showing video surveillance material that Salling in September 2019 sent an e-mail to all porters and parking guards associated with the company, who refers to the fact that only material from TV surveillance may be passed on to the police and thus not to other parties, and that this e-mail was reviewed at an office meeting with porters in the store in September 2019.

In addition, the Danish Data Protection Agency has emphasized that Salling has quoted the company's confidentiality agreements and employee handbooks to the Danish Data Protection Agency, which directly state that information may not be passed on to persons outside the company, that the company has guidelines for which persons may access the video surveillance. The company's guidelines for IT use state that the employees' non-compliance with the guidelines may have consequences for the employment relationship, including in the event of dismissal.

The Danish Data Protection Agency assesses that Saling cannot be considered responsible for an employee knowingly and against better knowledge in several ways, including by giving a former employee access to the building, has violated the company's guidelines. The Danish Data Protection Agency finds that the employee has taken up to several actions that go beyond what could reasonably be expected that Salling should have been prepared for or taken measures to avoid.

The Danish Data Protection Agency has further emphasized that the incident appears to be a limited and isolated incident that has occurred as a result of an abnormal action, and that both the sender and the recipient of the recordings have confirmed that they have deleted the information.

Against this background, the Danish Data Protection Agency finds that Salling's processing of personal data has taken place in accordance with Article 32 (1) of the Data Protection Regulation. 1.

The Danish Data Protection Agency has noted that the mentioned breach of personal data security has further resulted in the company asking all gatekeepers and parking guards to confirm in writing that they have read the applicable guidelines.

3.2. Article 33 of the Data Protection Regulation

It follows from Article 33 (1) of the Regulation 1, that the data controller in the event of a breach of personal data security without undue delay and if possible within 72 hours must report the breach to the Danish Data Protection Agency, unless it is unlikely that the breach of personal data security entails a risk to natural persons' rights or freedoms.

The Danish Data Protection Agency finds that Salling - by reporting the breach of personal data security 10 days after the company became aware of the incident - has not acted in accordance with Article 33 (1) of the Data Protection Regulation. 1.

In this connection, the Danish Data Protection Agency has emphasized that the recipient of the information made the Danish Data Protection Agency aware of the incident on 8 January 2020, and that Salling reported the breach of personal data security to the Danish Data Protection Agency on 18 January 2020. the deadline has not been met, as the case has been pending for further clarification of the facts, may lead to a different result.

3.3. Article 34 of the Data Protection Regulation

It follows from Article 34 (1) of the Regulation 1, that when a breach of personal data security is likely to involve a high risk to the rights and freedoms of natural persons, the data controller shall notify the data subject without undue delay of the breach of personal data security.

The Danish Data Protection Agency finds that Salling has acted in accordance with Article 34 (1) of the Data Protection Regulation. 1.

In this connection, the Danish Data Protection Agency agrees with what Salling stated that one of the two persons concerned was the one who made the company aware of the incident, and that there is no high risk to the rights or freedoms of the other person concerned.

3.4. Summary

On the basis of the above, the Danish Data Protection Agency finds that there is a basis for expressing criticism that Salling's processing of personal data has not taken place in accordance with Article 33 (1) of the Data Protection Regulation. 1.

In addition, the Danish Data Protection Agency finds that Salling's processing of personal data has taken place in accordance with Article 32 (1) of the Data Protection Ordinance. 1 and 34, para. 1.

[1] 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).