

Television surveillance of employees complied with GDPR

Date: 08-08-2022

Decision

Private companies

Serious criticism

Supervision / self-management case

Treatment safety

TV surveillance

In a case of its own initiative, the Danish Data Protection Authority has taken a closer look at Fitness World A/S' processing of employees' personal data.

Journal number: 2020-431-0115

Summary

On the basis of a number of specific inquiries from former employees, the Data Protection Authority initiated a case on its own initiative regarding, among other things, Fitness World A/S' television monitoring of employees.

TV surveillance was according to the rules

When you as an employer want to start television surveillance of the workplace, you must, among other things, ensure that there is a factual reason for it and that the monitoring is not more extensive than necessary. At the same time, as an employer, you must ensure that you provide employees with a range of information about the television surveillance - including the purpose of the surveillance and how long the recordings are kept. If the information is used to check on employees, the employer must remember that the employees must be informed about it in a clear and unambiguous way before such a check can take place.

In the specific case, the Data Protection Authority found no reason to criticize Fitness World's television surveillance of employees.

The Danish Data Protection Authority, however, expressed serious criticism of the fact that information about employees had been stored in a center in the form of e.g. medical certificates and resignations on a shared computer where the information had been accessible to other employees because it had been stored on the wrong drive.

Decision

The Danish Data Protection Authority hereby returns to the case, which the Danish Data Protection Authority has initiated on its own initiative regarding Fitness World A/S' (hereafter Fitness World) processing of personal data about employees.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that Fitness World's processing of personal data has not taken place in accordance with the data protection regulation[1] article 32, subsection 1.

The Danish Data Protection Authority also finds that Fitness World's processing of information about employees has taken place within the framework of Article 6, paragraph 1 of the Data Protection Regulation. 1, letter f, and article 14.

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

2. Case presentation

Through inquiries from former and current employees at Fitness World A/S, the Data Protection Authority became aware that Fitness World A/S conducts television surveillance of employees, and that the recordings have subsequently been used for, among other things, to give written warnings to employees. From the inquiries, it appears that the employees have not been informed about the purpose of the TV surveillance, including that recordings can be used as a control measure.

The inquiries also contained information that Fitness World A/S had not secured the employees' information sufficiently, as a local manager had downloaded and stored information about, among other things, resignations, contracts, written warnings, medical certificates and television surveillance recordings locally on a shared computer which was freely accessible to other employees. According to the inquiries, the information could also be accessed by members, as the computer was not "locked" after use.

In addition, according to what was stated, Fitness World A/S had also not sufficiently secured the members' information, as there was free access to the system "Exerp", where all information about members appears, as the computers were not "locked" after use, and the information was therefore free available to both employees and members.

The Danish Data Protection Authority decided to investigate the matter further on its own initiative and therefore requested Fitness World by letter of 23 November 2020 for an explanation in the matter. Fitness World appeared on 20 December 2020 with a statement on the matter. By letters of 25 May 2021 and 17 August 2021, the Danish Data Protection Authority requested

Fitness World for additional information, which Fitness World provided on 6 July 2021 and 30 August 2021.

2.1. Fitness World's comments

2.1.1.

Fitness World has generally stated that television surveillance is carried out in all of Fitness World's centers in order to prevent crime, increase the safety of employees and members, and to prevent gross violations of Fitness World's internal rules.

Fitness World has stated that the legal basis for the processing is the data protection regulation's article 6, subsection 1, letter f, as well as article 10, cf. sections 6 and 8 of the Data Protection Act. Fitness World has a legitimate interest in televising e.g. entrance areas, reception areas, fitness areas and training halls in order to prevent and solve crime, security and insurance reasons and to be able to assert legal claims in connection with employment.

Signs about television surveillance have been erected at the entrances, and employees are informed about television surveillance in the employment contract, the staff handbook, the personal data policy for employees and Fitness World's policy on television surveillance. From Fitness World's policy on television surveillance - which is provided upon employment - employees are informed about the purpose of the television surveillance and that the places where Fitness World has chosen to carry out television surveillance are marked with clear signs before entering the monitored area, e.g. at entrance doors. The employees are also informed that there is no TV surveillance in changing areas or at toilet facilities.

Recordings are stored for a maximum of 21 days, after which they are deleted when overdubbed. In specific cases, extracts of the recordings are kept to the extent that there is a basis for this in the legislation, after which they are deleted.

The television surveillance is reviewed in the form of random checks in case of specific suspicions or other irregularities. In relation to employees, this may be the case in the event of gross violations of Fitness World's internal rules, e.g. theft or internal embezzlement, harassment, violence or systematic cheating with time registration. Fitness World has further stated that, as a rule, "live" TV monitoring is not followed, but if there is a concrete suspicion, it is an option to follow "live". In relation to the specific cases, Fitness World has not been able to establish that there should have been "live" TV monitoring.

Fitness World has further stated that a guide is issued to all managers in local centers with information about television surveillance, where it is stated that as a manager you must not use television surveillance to check whether employees are doing their work correctly. Furthermore, it appears that misuse of television monitoring will be in breach of Fitness World's personal data policy and may trigger a warning or dismissal as a manager. Furthermore, it appears from the instructions to the

center managers that if a manager has a legitimate reason for wanting to see television surveillance, the managers must contact HR for an assessment of the matter.

Only the security department at Fitness World's head office has access to television surveillance recordings, and recordings are only released to center managers if a specific written request is received. In relation to the specific cases, Fitness World has not been able to establish that there should have been a request for the release of recordings. Only the security department has access to download material from the servers. If the material has been obtained in the event of crime, the material is sent directly from the security department to the police, and if the material relates to internal matters, the material is sent directly from the security department to HR.

In relation to the specific episodes that the Danish Data Protection Authority has received inquiries about - where a center manager has saved television surveillance recordings of some of the center's employees - Fitness World has stated that the recordings originate from 2018 and that the procedure for handling television surveillance subsequently has been changed so that recordings from TV surveillance can no longer be saved locally or downloaded by a manager. In relation to the specific episodes, there has been an error on the part of the manager, which has been reported and dealt with internally, and the individual manager's access to request the release of surveillance material has also been significantly restricted.

2.1.2.

Regarding processing security, Fitness World has stated that all computers in Fitness World are protected with a personal login and password, and that access to personal data in the Exerp system and on the computers is otherwise isolated to employees with a work-related need to be able to access this personal data. Access is adapted to the individual's position and with a personal password, and the systems operate with automatic log out.

Fitness World has stated that upon employment, staff are instructed on the correct use of computers, including locking the computer when they leave it, and that there is written material on information security in several different policies – including the security policy in connection with personnel administration and the employee handbook. In the on boarding process for new employees, a GDPR module is also taught about, among other things, IT security.

Previously, Fitness World's computers contained a shared center mailbox accessible to all employees and a manager mailbox reserved only for the manager of the center. Documents such as resignation files, contracts, written warnings, medical reports and television surveillance were always sent to the manager mailbox. According to the information, login to the manager's

mailbox took place via a separate browser and with a personal password.

In relation to the inquiries that the Danish Data Protection Authority has received that personnel information has not been adequately secured, Fitness World has stated that the manager of the center had unfortunately saved documents on the wrong drive, which is not acceptable and which Fitness World regrets. It has been a management error, which has subsequently been corrected so that it cannot happen again.

On the occasion of the Data Protection Authority's request, all managers in the centers have now been assigned personal computers with a personal username and password for both the computer and the individual systems, where information about terminations, contracts, written warnings, medical reports etc. is located, so that all information about employees is now stored securely on a computer associated with a manager and not on a common computer in the centre.

According to Fitness World, information about employees has never been freely available to members, as all Fitness World's systems require employee login with a password, and staff are instructed upon employment on the correct use of computers, including locking the computer when the employee leaves it, and also "locking" the computers automatically. All employees who handle information about a colleague are also informed of the guidelines for this as described in Fitness World's security policy in connection with personnel administration.

Fitness World has also pointed out that work is being done on further separation of employee access in relation to function, so that the company achieves a better distribution between shared access and individual access. Furthermore, a systematic review of the centers is initiated with a view to checking each individual center's compliance with the personal data policy and the information security policy. Fitness World is also working to tighten the security measures in connection with employees' use of computers, including training and reminders about the correct use of computers. Fitness World will also prepare new and more comprehensive teaching material both for on-boarding of new employees as well as ongoing compulsory further training.

3. Reason for the Data Protection Authority's decision

3.1. TV surveillance of employees – control measure

The rules in the Data Protection Regulation and the Data Protection Act apply to any form of processing of personal data in connection with television surveillance. Authorization for the processing can be found in § 12, subsection of the Data Protection Act. 1, whose processing takes place as part of a control measure in accordance with a collective agreement on

control measures. If the measure is not regulated in such an agreement, the authority for the processing will have to be found in either the data protection regulation, article 6, subsection 1, letter e (exercise of authority), or Article 6, subsection 1, letter f (the balancing of interests rule).

Furthermore, the processing can only take place if the basic processing principles in the regulation's article 5 on i.a. legality, reasonableness and transparency, purpose limitation and storage limitation are met. This means, among other things, that an employer can carry out television surveillance at a workplace if there is a factual reason for it, and the surveillance is not more extensive than necessary.

In addition, it follows from articles 13 and 14 of the data protection regulation that data controllers have a duty to provide a range of information to the data subject when information is processed about him. The employees must, among other things, receive information that television surveillance is being carried out, the purpose of the television surveillance, and in which cases the footage can be reviewed and passed on to the police. As a rule, the information must be provided in advance, and new employees must be notified in connection with their employment, or at the latest when they start working in TV-monitored premises.

In the case of the employer's processing of personal data in connection with control measures against the employees, the principle of transparency in the data protection regulation, Article 5, subsection 1, letter a, that the employer must, as a starting point, give the employees prior information about the control measures used, including in particular about the purpose of the control.

Based on the information in the case, the Danish Data Protection Authority assumes that Fitness World processes information about the company's employees in the form of television surveillance for crime prevention and investigation purposes and to be able to assert legal claims against the employees.

The Danish Data Protection Authority also assumes that Fitness Worlds' television monitoring of the employees does not take place in accordance with a collective agreement on control measures, and that, as a clear starting point, only information covered by Article 6 of the Data Protection Regulation is processed.

The Danish Data Protection Authority finds no basis for overriding Fitness World's assessment that the processing of information about employees in the form of television surveillance can be done on the basis of Article 6, paragraph 1 of the Data Protection Regulation. 1, letter f.

The Danish Data Protection Authority has thereby emphasized that the processing is carried out with a view to preventing crime and to secure evidence and thus information for use by the police in the event of crime, and to be able to enforce any legal claims against the employees.

On the basis of Fitness World's information in the case, the Danish Data Protection Authority also assumes that employees in connection with their employment have been informed about the television surveillance and the purposes thereof - including that the purpose i.a. is to be able to assert legal claims against the employees - which is why the supervisory authority does not find grounds to conclude that the processing should have taken place in violation of Article 14 of the Data Protection Regulation.

3.2. Treatment safety

Article 32, subsection of the Data Protection Regulation. 1, states that the data controller, taking into account the current technical level, the implementation costs and the nature, scope, context and purpose of the processing in question as well as the risks of varying probability and seriousness to the rights and freedoms of natural persons, implements technical and organizational measures to ensure a level of security appropriate to these risks.

In relation to the processing of information about Fitness World's members, the Danish Data Protection Authority finds no basis for concluding that Fitness World has not sufficiently implemented appropriate security measures. In this connection, the Danish Data Protection Authority emphasized that members' information - based on the information provided - could not be accessed by members, as the computers were "locked" after use.

However, it appears from the case that Fitness World has stored information about a number of employees in the form of medical certificates, resignations, contracts and written warnings as well as television surveillance images on a shared computer, where the information has been available to other employees because it was stored on a wrong drive.

In this connection, the Danish Data Protection Authority's assessment is that a shared computer, which is used by both employees for daily use and by managers for handling information about terminations, contracts, written warnings, medical reports, etc., constitutes a proximate risk for those registered - in this case the employees' rights.

The Danish Data Protection Authority therefore considers that there are grounds for expressing serious criticism that Fitness World's processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1.

In the specific case, the Danish Data Protection Authority emphasized that the use of the shared computer entailed the passing on of medical reports, resignations, contracts and written warnings as well as television surveillance images between the employees.

The Danish Data Protection Authority has noted that managers in Fitness World's centers have subsequently been assigned personal computers with personal logins to both the computer and the individual systems, and that

Fitness World has also ensured more training for employees, i.a. an education which is particularly aimed at local leaders.

[1] 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 and on the repeal of Directive 95/46/EC (general regulation on data protection).