

Supervision of the House of Boards

Date: 07-08-2020

Decision

Public authorities

Journal number: 2019-421-0034

Summary

In August 2020, the Danish Data Protection Agency completed a planned written inspection at Nævnenes Hus. The audit focused on the Boards of the Board's compliance with the rules on the duty to provide information when using control measures towards employees. The audit also focused on whether the House of Commons' observance of the duty to provide information complied with the regulation's basic principle of transparency, which, among other things, implies that the data controller must provide employees with easily accessible and prior information about the control measures applied.

On the basis of the audit carried out, the Danish Data Protection Agency has had occasion to express criticism of the Board of Directors' processing of personal data.

The Danish Data Protection Agency's concluding statement states, among other things, that the Board's compliance with the duty to provide information has been deficient in several cases, including that the authority has not provided employees with sufficiently clear information about the data controller's identity, purpose of processing the information. the categories of personal data concerned, any recipients or categories of recipients of the data, and the period during which the data will be stored or, if this is not possible, the criteria used to determine this period.

You can read the Danish Data Protection Agency's guide on data protection in connection with employment relationships [here](#).

You can read the Danish Data Protection Agency's guide on data subjects' rights [here](#).

Decision

1. Written supervision of the Board of Trustees' processing of personal data

The House of Boards was among the authorities that the Danish Data Protection Agency had chosen to supervise in the autumn of 2019 in accordance with the Data Protection Ordinance [1] and the Data Protection Act [2].

The Danish Data Protection Agency's audit was a written audit that focused on the Board's compliance with the duty to provide information in connection with control measures towards employees, cf. Articles 13 and 14 of the Regulation. in Article 5 (1) of

the Regulation. 1, letter a, which according to the Authority's assessment i.a. implies that the data controller must provide employees with easily accessible - prior - information about the control measures used.

By letter dated 9 September 2019, the Danish Data Protection Agency notified the Authority of the Board of Trustees and in this connection requested the authority for an opinion.

The House of Boards has subsequently issued a statement by letter dated 4 October 2019 for use in the case.

Following the audit of the House of Boards, the Danish Data Protection Agency finds reason to conclude:

That the Board of Trustees' compliance with the duty of disclosure under Articles 13 and 14 of the Regulation has been deficient in several cases, including in that the authority has not provided employees with sufficiently clear information about the identity of the data controller, the purpose of processing the information, the legal basis for the processing, categories of personal data, any recipients or categories of recipients of the data, and the period during which the data will be stored, or if this is not possible, the criteria used to determine this period.

The Danish Data Protection Agency then finds grounds for expressing criticism that the Board of Directors' processing of personal data has not taken place in accordance with Articles 13 and 14 of the Data Protection Ordinance. of personal data has not been done in accordance with the basic principle of transparency in Article 5 (1) of the Regulation. 1, letter a.

Below is a more detailed review of the information that has emerged in connection with the written inspection and a justification for the Danish Data Protection Agency's decision.

2. The Board's House 'use of control measures towards employees

The Board of Trustees has informed the Danish Data Protection Agency that the authority makes use of the following control measures against employees:

TV surveillance in certain areas.

Logging of employees' opening of locked doors when doors are opened from the outside.

Logging of employees' actions in the authority's ESDH system.

Registration of employees' working hours.

Central logging of the employees' work computer.

In this connection, the House of Boards has stated that all the authority's employees are affected by the above-mentioned control measures, and that the authority does not make use of individual control measures against individual employees or

groups of employees.

3. Procedures, etc. in relation to the fulfillment of the duty to provide information and prior information on control measures

The Board of Trustees has stated that the authority's employees are informed about the processing of personal data in connection with the use of control measures via the authority's internal privacy policy and associated appendices. The privacy policy is handed out to new employees on their first working day as part of the welcome package and can otherwise be accessed by all employees on the intranet.

In this connection, the House of Boards has stated that the authority has prepared a checklist to be used when hiring new employees. However, the checklist has only been prepared on 20 September 2019, which is after the date of the Danish Data Protection Agency's notification of the audit on 9 September 2019. It appears, among other things, of the checklist that the responsible parking manager or partner must hand over a copy of the Board of Trustees' current privacy policy (and associated appendices) to the new employee.

The Board of Trustees has sent a copy of the authority's privacy policy and the two annexes thereto, which are used for the authority's compliance with Articles 13 and 14 of the Data Protection Regulation in connection with control measures against employees. It appears that the privacy policy and the associated appendices have been prepared before the Danish Data Protection Agency's notification of the audit.

One appendix to the privacy policy concerns notification of the processing of personal data by the Ministry of Business Affairs' Group HR. The second appendix concerns logging of certain actions at Statens IT (SIT).

The Privacy Policy and its annexes are reviewed below in Section 4.

The Board of Trustees has stated that the privacy policy and the associated appendices will be revised immediately if new control measures are introduced, and that employees will be informed of the revised policy per. e-mail, at a house meeting and with a news item on the Board of Trustees' intranet.

It is the Data Inspectorate's assessment that - pursuant to the principle of legality, reasonableness and transparency pursuant to Article 5 (1) of the Data Protection Regulation. 1, letter a - as a starting point, prior information must be provided on the use of control measures. In the Authority's view, when implementing new control measures, the employer must, as a general rule, inform employees of the control measures no later than 6 weeks before they are implemented. [3]

The Danish Data Protection Agency must therefore recommend that the Board of Trustees - if the authority is not already

aware of this - informs employees in future of new control measures no later than 6 weeks before they are implemented. In the Authority's view, this could constitute a breach of the principle of transparency within the meaning of Article 5 (1) of the Regulation. 1, letter a, if employees are first notified of new measures upon their introduction without a factual justification for this.

4. Review of the Board of Trustees' privacy policy and associated appendices

In connection with the inspection, the House of Boards has submitted the latest two versions of the authority's privacy policy. In this connection, the Danish Data Protection Agency must draw attention to the fact that the Authority has only taken a position on the version of the privacy policy that was in force on the date of the notification of the Authority.

The Board of Trustees has stated [4] that the authority makes use of a number of control measures - which can be used for both security and control purposes - towards the authority's employees. The Danish Data Protection Agency can not rule out that these are used for control purposes against the authority's employees, which is why this is the basis for the review of the privacy policy and the associated appendices.

The Danish Data Protection Agency presupposes that the Board of Trustees is responsible for data in connection with the control measures that the authority has stated it will use.

4.1. Regarding information on TV surveillance

Regarding the use of television surveillance as a control measure, it appears, among other things, of the privacy policy that television surveillance is carried out in specific areas. In addition, it appears that the television surveillance material is stored in safe environments and with limited access, and that employees in a particular department are responsible for reviewing television surveillance material when there is a factual justification for this. Finally, it appears that the TV surveillance material is deleted after 30 days.

It follows from section 3 b of the Television Surveillance Act [5] that the provision in Article 14 of the Data Protection Regulation applies regardless of any signage pursuant to sections 3 and 3 a of the Act. comply with the requirements of Article 14 of the Data Protection Regulation.

Following a review of the privacy policy, the Danish Data Protection Agency's assessment is that the section on television surveillance does not provide employees with sufficient information about the purpose of the processing for which the personal data is to be used, as the purpose statement is not precise enough in relation to the control purpose.

In addition, it is the Authority's assessment that employees are not given information about the legal basis for the processing and the affected categories of personal data.

Overall, the Danish Data Protection Agency finds that Nævnenes Hus' notification of the processing of personal data in connection with television surveillance of employees in certain areas does not live up to the requirements of Article 14 (1) of the Data Protection Ordinance. 1, letters c and d.

Considering that, in the opinion of the Danish Data Protection Agency, the purpose of the control has not been sufficiently transparent for the employees, the Authority also finds that the Board's information on television surveillance has not complied with the basic principle of transparency in Article 5 (1) of the Regulation. 1, letter a. In this connection, the Danish Data Protection Agency must also emphasize that it is the Authority's assessment that the principle of transparency i.a. implies that the data controller must provide employees with easily accessible - prior - information about the control measures used, including in particular about the control purpose.

To the extent that there will be recipients of the information collected about employees in connection with television surveillance, the Danish Data Protection Agency must draw attention to the fact that the notification must contain information about this, cf. Article 14 (1) of the Regulation. 1, letter e.

4.2. Regarding information on logging the employees' opening of locked doors

It appears from the privacy policy that the employees' access card number and time are logged when employees open a locked door with their access card. In addition, it appears that the log information is stored in secure environments and with limited access, and that employees in a specific department can request the information when there is a factual justification for this. As an example of this, it appears that the information can be requested in cases where there have been problems with an alarm in the evening due to lack of shutdown, and that the department in question therefore wants to contact the employee in question to instruct him to set the alarm correctly. .

As the Danish Data Protection Agency's personal data is collected from the employee himself when he uses his access card, the Authority's assessment is that notification of the processing of personal data in connection with logging employees' entrance of locked doors must comply with the requirements of Article 13 of the Data Protection Regulation.

Following a review of the privacy policy's information on logging employees' entry of locked doors, the Danish Data Protection Agency is of the opinion that the employees will not be given information on the purpose of the processing of the log

information in question and the legal basis for the processing. The Danish Data Protection Agency hereby emphasizes that, in the Authority's opinion, it is not clear from the notification that the log information in question can also be used for control purposes against the employees.

In addition, it is the Data Inspectorate's assessment that employees are not given information about the period during which the log information will be stored, or if this is not possible, the criteria used to determine this period. The Danish Data Protection Agency has hereby emphasized that this information - in the Authority's view - is necessary to ensure fair and transparent processing as far as the employees are concerned.

Overall, the Danish Data Protection Agency finds that Nævnenes Hus' notification of the processing of personal data in connection with logging of employees' entrance of locked doors does not live up to the requirements of Article 13 (1) of the Data Protection Ordinance. Article 13 (1) (c) and Article 13 (1) 2, letter a.

In view of the fact that, in the opinion of the Danish Data Protection Agency, the control purpose has not been sufficiently transparent for employees, the Authority also finds that the Board's information on logging employees' entrance of locked doors has not complied with the basic principle of transparency in Article 5 (1) of the Regulation. 1, letter a. In this connection, the Danish Data Protection Agency must also emphasize that it is the Authority's assessment that the principle of transparency i.a. implies that the data controller must provide employees with easily accessible - prior - information about the control measures used, including in particular about the control purpose.

4.3. Regarding information on logging employees' actions in the authority's ESDH system

It appears from the privacy policy that logging takes place in Nævnenes Hus' ESDH system when employees open, edit, copy or move files. In addition, it appears that random samples are taken from the log at regular intervals with the aim of documenting checks that files are only accessed when there is a work-related need for them. The starting point for the control is that there will be a work-related need to access files in cases with the board / boards to which the employee has access rights.

It is also here that the Danish Data Protection Agency's assessment that notification of the processing of personal data in connection with logging of employees' use of the ESDH system must live up to the requirements of Article 13 of the Data Protection Ordinance.

After a review of the privacy policy, it is the Data Inspectorate's assessment that employees are not given information about

the legal basis for the processing. It is also the Data Inspectorate's assessment that employees are not given information on the period during which the log information will be stored, or if this is not possible, the criteria used to determine this period, which - in the Authority's view - is necessary information to ensure a fair and transparent treatment as far as the employees are concerned.

The Danish Data Protection Agency thus finds that the Board's House's notification of the processing of personal data in connection with logging in the authority's ESDH system does not live up to the requirements of Article 13 (1) of the Data Protection Regulation. Article 13 (1) (c) and Article 13 (1) 2, letter a.

4.4. Regarding information on registration of employees' working hours

Regarding time registration, it appears from the privacy policy that the employee's information in the time registration system is processed by Group HR, and reference is therefore made to the appendix the notification on processing information with Group HR. Furthermore, it appears from the privacy policy that the employee's time registration information is processed by his or her personnel manager in connection with the monthly approval of the time registration. Finally, it appears that the information is stored in secure environments, and that individual employees in the administration and the employee's theme manager have access to the information, just as it appears that the information is anonymised and aggregated through statistical processing so that it is not personally identifiable.

From the appendix with the notification of processing information at Group HR, it appears regarding the time registration information that information about the employee's initials, full name, social security number, B-number (regarding access to IT systems), workplace, standard working hours, the employee's area / center is processed. nearest boss and any children's name and birthday, as well as information on absence is processed. In addition, it appears that this information can be accessed by Group HR, the employee's local time registration manager, the local finance department and the person's manager. Furthermore, it appears, among other things, that a number of the information mentioned may be passed on to specific recipients. Finally, the notification describes how long the information in question is stored.

It is the Data Inspectorate's assessment that notification of processing of personal data in connection with the Board's House 'processing of information on employees' time registration must live up to the requirements in Article 13 of the Data Protection Ordinance, as the data is collected by the employee himself .

Following a review of the privacy policy and the notification of processing of information by Group HR, it is the Data

Inspectorate's assessment that the employees are not given sufficient information about the purpose of the processing of the information in question and the legal basis for the processing. The Danish Data Protection Agency hereby emphasizes that, in the Authority's view, it is not sufficiently clear from the notification that the time registration information in question can be used for control purposes against the employees.

On this basis, the Danish Data Protection Agency finds that the Board of Trustees' notification of the processing of personal data in connection with the registration of employees' working hours does not live up to the requirement in Article 13 (1) of the Data Protection Ordinance. 1, letter c.

Considering that, in the opinion of the Danish Data Protection Agency, the control purpose has not been sufficiently transparent for the employees, the Authority also finds that the Board's information on registration of the employees' working hours has not complied with the basic principle of transparency in Article 5 (1) of the Regulation. 1, letter a. In this connection, the Danish Data Protection Agency must also emphasize that it is the Authority's assessment that the principle of transparency i.a. implies that the data controller must provide employees with easily accessible - prior - information about the control measures used, including in particular about the control purpose.

4.5. Regarding information about central logging of the employees' work computer

An appendix to Nævnenes Hus' privacy policy concerns central logging of the employees' work computer carried out by Statens IT. It appears i.a. of which the purpose of the logging of the work computer is to give Statens IT the opportunity to make machine analyzes if a breach of security is found. In addition, it appears which specific information is registered in the log. It further appears that the information is pseudonymised, but that it is possible to remove the pseudonymization if it is strictly necessary in connection with some exemplified security incidents. In conclusion, it appears that only a few authorized employees in Statens IT have access to information that identifies individuals, and that no one in the Boards' House will have access to the registered information. The log is stored for 18 months, based on the police instructions for storing security logs. In the opinion of the Data Inspectorate, as the personal data is collected from the employee himself when he uses his work computer, the Authority's assessment is that notification of the processing of personal data in connection with central logging of employees' work computers must comply with Article 13 of the Data Protection Regulation.

After a review of the privacy policy and the attached appendix, it is the Data Inspectorate's assessment that the employees are not given sufficiently clear information about the data controller's identity. The Danish Data Protection Agency emphasizes that

it appears from Nævnenes Hus' privacy policy that the authority has no influence on - or access to - the processing of information carried out by Statens It. As the Danish Data Protection Agency assumes that the Board of Trustees is data responsible in connection with the control measures that the authority has stated that it will make use of, the Board finds that - in view of the above wording - it is not sufficiently clear to the employees that the Board of Trustees is the data controller in connection with this processing of personal data.

In addition, the Authority's assessment is that the employees will not be given information about the purpose of the processing of the information in question and the legal basis for the processing. In this connection, the Danish Data Protection Agency emphasizes that, in the Authority's view, the purpose statement is not precise enough in relation to the control purpose.

The Danish Data Protection Agency thus finds that Nævnenes Hus 'notification of the processing of personal data in connection with central logging of employees' work computers does not live up to the requirement in Article 13 (1) of the Data Protection Ordinance. 1, letters a and c.

In view of the fact that the control purpose, in the opinion of the Danish Data Protection Agency, has not been sufficiently transparent for employees, the Authority also finds that the Board's House's information on central logging of employees' work computers has not lived up to the basic principle of transparency in Article 5 para. 1, letter a. In this connection, the Danish Data Protection Agency must also emphasize that it is the Authority's assessment that the principle of transparency i.a. implies that the data controller must provide employees with easily accessible - prior - information about the control measures used, including in particular about the control purpose.

5. Conclusion

Following the audit of the House of Boards, the Danish Data Protection Agency finds reason to conclude:

That the Board of Trustees' compliance with the duty of disclosure under Articles 13 and 14 of the Regulation has been deficient in several cases, including in that the authority has not provided employees with sufficiently clear information about the identity of the data controller, the purpose of processing the information, the legal basis for the processing, categories of personal data, any recipients or categories of recipients of the data, and the period during which the data will be stored, or if this is not possible, the criteria used to determine this period.

The Danish Data Protection Agency then finds grounds for expressing criticism that the Board of Directors' processing of personal data has not taken place in accordance with Articles 13 and 14 of the Data Protection Ordinance. of personal data

has not been complied with in accordance with the fundamental principle of transparency set out in Article 5 (1) of the Regulation. 1, letter a.

[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

on the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46 / EC (General Data Protection Regulation).

[2] Act No. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

[3] Reference is made to the Danish Data Protection Agency's guidelines on data protection in connection with employment relationships, section 7, which can be accessed on the Authority's website:

<https://www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger/>

[4] See Section 2 of the Decision

[5] Statutory Order no. 1190 of 11 October 2007 on television surveillance with subsequent amendments