The Norwegian Data Protection Authority expresses serious criticism of the Danish Society for Acute Medicine's processing of personal data

Date: 13-12-2021

Decision

Private companies

Serious criticism

Complaint

Treatment safety

The Danish Data Protection Authority has made a decision in a case where board members of the Danish Society for Acute Medicine processed personal data on private computers and e-mail accounts.

Journal number: 2021-31-4497

Summary

On 13 December 2021, the Danish Data Protection Authority made a decision in a case concerning the Danish Society for Acute Medicine's processing of personal data on board members' private computers and e-mail accounts.

After the case had been submitted to the Data Council, the Data Protection Authority stated that the Danish Society for Acute Medicine had not taken appropriate organizational and technical measures.

The supervisory authority laid, among other things, emphasis on the fact that it follows from the requirement for adequate security that associations or organizations that allow board members to process personal data for which the association or organization is the data controller must implement appropriate security measures in connection with this.

It must therefore be possible to check that the board members comply with the security measures that the association or organization as data controller has decided to implement when they process personal data. In addition, the association or organization must also - where relevant - set guidelines and procedures for board members' use of the equipment.

The Danish Data Protection Agency could agree with the Danish Society for Acute Medicine's own assessment that the company had not had a sufficient level of security for personal data received through external inquiries.

Against this background, the Danish Data Protection Authority found grounds to express serious criticism that the Danish Society for Acute Medicine's processing of personal data has not taken place in accordance with the rules in the data

protection regulation.

1. Decision

The Data Protection Authority hereby returns to the case where the complainant complained to the Authority on 13 January 2021 about the Danish Society for Acute Medicine's processing of personal data.

The Danish Data Protection Authority has understood the complainant's inquiry as a complaint that the Danish Society for Acute Medicine's processing of information about complaints is not secure, as the processing takes place on the private computers and e-mail accounts of the company's board members.

After a review of the case, the Danish Data Protection Authority finds - after the case has been submitted to the Data Council - that there is a basis for expressing serious criticism that the Danish Society for Acute Medicine's processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 32, PCS. 1.

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

2. Case presentation

It appears from the case that the Danish Society for Acute Medicine has the right to be consulted when processing job applications regarding positions as an expert in the Patient Complaints Agency.

It also appears that in autumn 2019 the complainant sent a job application to the Agency for Patient Complaints. In connection with the assessment of the application, the job application was sent to the Danish Society for Emergency Medicine for an opinion.

The complainant subsequently objected to the Danish Society for Acute Medicine's decision not to recommend the complainant for employment with the Agency for Patient Complaints.

In this connection, the complainant was informed that the chairman of the Danish Society for Acute Medicine would look into the complainant's case, but that it was on the chairman's private e-mail account, and the complainant therefore had to wait for a reply from the chairman.

2.1. Complainant's comments

The complainant stated that he received a reply to his objection from the Danish Society for Acute Medicine's chairman's private e-mail address. In this connection, the complainant has indicated that he does not think it is justifiable that information in application cases in connection with the Danish Society for Acute Medicine's consultation right in these cases is stored and

processed on private computers and e-mail accounts belonging to the company's board members.

2.2. Danish Society for Emergency Medicine comments

The Danish Society for Acute Medicine has generally stated that the Agency for Patient Complaints, when processing job applications regarding positions as an expert in the agency, where the Danish Society for Acute Medicine has the right to be consulted, usually writes to the company's official e-mail address, which is set up so that it automatically forwards the e-mail to the private e-mail account of the chairman of the Danish Society for Acute Medicine. There is thus no independent mailbox linked to the Danish Society for Acute Medicine's official e-mail address.

As far as the specific case is concerned, the Danish Society for Acute Medicine has stated that the company's chairman replied to the Agency for Patient Complaints from his private e-mail address. In this connection, the Danish Society for Acute Medicine has stated that the Danish Society for Acute Medicine has no other email systems to respond from, and the company also does not have a special computer standing by to answer such inquiries.

The Danish Society for Acute Medicine has also stated that all board members use their own private computers and e-mail accounts for board work, and that it was not the Danish Society for Acute Medicine's view that the actual ownership of the computers in question had any significance for data security.

In addition, the Danish Society for Acute Medicine has stated that in connection with the processing of the complainant's information, the company's chairman's private computer and e-mail account were password protected. In this connection, the Danish Society for Acute Medicine has stated that the chairman's e-mail system uses TLS version 1.2. In this connection, the Danish Society for Acute Medicine assessed that the information exchanged with the Agency for Patient Complaints was not of such a nature that further encryption was required.

Dansk Selskab for Akutmedicin has subsequently stated that, in connection with the present case, the company has become aware that Dansk Selskab for Akutmedicin has not had a sufficient level of security for the processing of personal data received from external inquiries. The Danish Society for Acute Medicine has stated that in future the company will ensure that external inquiries go directly to the Danish Society for Acute Medicine's e-Box.

3. Reason for the Data Protection Authority's decision

3.1.

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, must implement technical and organizational measures in order to ensure a level of security appropriate to these risks.

The Norwegian Data Protection Authority finds – after the case has been submitted to the Data Council – that it follows from the requirement for adequate security, cf. Article 32, that associations or organizations that allow board members to process personal data for which the association or organization is the data controller must implement appropriate security measures in connection herewith.

The Danish Data Protection Authority is of the opinion that security measures should basically contain elements of physical security, organizational conditions, system technical conditions, as well as training, instruction and control.

The Danish Data Protection Authority can also refer to the guidance on voluntary associations' processing of personal data, which the Ministry of Justice prepared in December 2018 with the involvement of the Danish Data Protection Authority, and which is available via the Danish Data Protection Authority's website[2]. In the guide, the Ministry of Justice provides answers to a number of frequently asked questions that can help voluntary associations and organizations comply with the rules in the Data Protection Regulation and the Data Protection Act.

In the opinion of the Danish Data Protection Authority, associations or organizations must thus instruct the board members and be able to monitor that the processing of personal data carried out by the board members takes place in compliance with the security measures that the association or organization as the data controller has decided to implement. Examples of this could be access control, encryption of data and other technical security measures on the equipment and e-mail accounts that the board members of the association or organization use in the performance of their duties. In addition, the association or organization must also - where relevant - set guidelines and procedures for board members' use of the equipment.

In the Danish Data Protection Authority's opinion, the above also applies in principle if the association or organization – as is the case in this case – allows the board members to use their own private equipment and e-mail accounts to process the personal data. In this connection, however, the Danish Data Protection Authority understands that the structure of the association can make such a power of instruction and control difficult in practice.

In the Data Protection Authority's view, it will e.g. be difficult for a data controller to control the security under which board members process personal data on their private computers, such as, for example, which access control the individual board

member has on his private computer, as well as how the board member stores or transports his private computer, and how the security of the private computer may be configured or how many potentially harmful applications are installed.

In view of this, the Danish Data Protection Authority is of the opinion that in cases such as in the present case, where the processing of personal data to be carried out consists of the assessment and communication of confidential or sensitive information, a solution must be established which ensures that this confidentiality does not undermined. Thus, sensitive or confidential personal data may not be sent unencrypted over networks over which the data controller does not have full control, e.g. unencrypted e-mail on the Internet. In these situations, a safe solution must be used. This could, for example, be use of the association's e-Boks, common association portal with differentiated access or use of an internal mail client with the necessary security, e.g. in the form of separate e-mail accounts with individual access for those who process personal data and the possibility of necessary encryption for sending and receiving e-mail.

In this connection, control can, for example, consist of the data controller continuously inquiring and ensuring that the processing of personal data takes place in compliance with the security measures that have been established, including that the data controller continuously reminds and ensures that the board members comply with the established requirements for e.g. updating anti-virus programs, deleting data or the like.

3.2.

On the basis of the information in the present case, the Danish Data Protection Authority assumes that the Danish Society for Emergency Medicine had not drawn up any formalized procedures or guidelines for how the processing of personal data on the board members' private computer and e-mail accounts could take place with appropriate security, including e.g. e.g. requirements for access control, virus scan, deletion of data or the like.

Based on this, the Data Protection Authority finds that the Danish Society for Emergency Medicine has not taken appropriate organizational and technical measures to ensure a level of security that was suitable for the risks involved in the association's processing of personal data, cf. the data protection regulation, article 32, subsection 1.

The Danish Data Protection Authority can thus agree with the Danish Society for Acute Medicine's own assessment that the company has not had a sufficient level of security for personal data received through external inquiries.

The Danish Data Protection Authority therefore finds grounds for expressing serious criticism that the Danish Society for Acute Medicine has not met the requirements for an appropriate level of security in the data protection regulation, article 32,

paragraph. 1.

The Danish Data Protection Authority has noted that the Danish Society for Emergency Medicine will in future use e-Boks for external communication.

4. Concluding remarks

The Data Protection Authority's decisions cannot be appealed to another administrative authority, cf. Section 30 of the Data Protection Act.

The Data Protection Authority's decisions can, however, be appealed to the courts, cf. § 63 of the Basic Law.

[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).

[2].