Supervision of Region Nordjylland's issuing of access cards

Date: 18-01-2022

Decision

Public authorities

No criticism

Supervision / self-management case

Access control

Treatment safety

The Data Protection Authority has overseen the North Jutland Region's procedures for issuing access cards for the region's hospitals and premises where personal data is processed.

Journal number: 2021-422-0033

Summary

Region North Jutland was among the authorities that the Data Protection Authority supervised in the first half of 2021.

The inspection was a written inspection which focused on the North Jutland Region's procedures for issuing access cards to the region's hospitals and premises where personal data is processed.

In connection with the processing of the case, the Data Protection Authority received, among other things, Region Nordjylland's guidelines on the allocation and issuance of access cards.

The Norwegian Data Protection Authority found that there was no basis for overriding the region's assessment that the initiated procedures for issuing access cards constitute appropriate security measures.

In this connection, the Danish Data Protection Authority emphasized that the North Jutland Region uses access control to locked rooms, that the region has procedures for issuing access cards, and that the region also has other security measures to prevent unauthorized persons from gaining access to personal data at the region's locations.

Decision

1. Written supervision of Region Nordjylland's processing of personal data

Region North Jutland was among the authorities that the Data Protection Authority had selected in the first half of 2021 to supervise according to the data protection regulation[1] and the data protection act[2].

The Danish Data Protection Authority's inspection was a written inspection which focused on the North Jutland Region's procedures for issuing access cards to the region's hospitals and premises where personal data is processed.

By letter of 11 June 2021, the Norwegian Data Protection Authority notified the Norwegian Supervisory Authority for Region North Jutland and requested an opinion in this regard. Region Nordjylland issued a statement on the matter on 2 July 2021.

On 14 September 2021, the Data Protection Authority requested a supplementary opinion, which Region Nordjylland issued on 29 September 2021.

2. The Data Protection Authority's decision

After a review of the case, the Data Protection Authority finds that there is no basis for overriding Region Nordjylland's assessment that the procedures implemented for issuing access cards to the region's hospitals and premises in which personal data is processed constitute appropriate security measures, cf. Article 32 of the Data Protection Regulation.

Below follows a closer review of the information that has come to light in connection with the written inspection and a justification for the Data Protection Authority's decision.

3. Disclosure of the case

Region North Jutland has stated that the region's hospitals are by nature open buildings, where patients and relatives move around in the vast majority of the buildings. Access cards are used i.a. for ID cards, so that patients and relatives can identify the employees. In addition, the cards give the employees access to e.g. follow me print and locked rooms, e.g. medicine room and operating room.

It appears from Region Nordjylland's general page on the region's intranet about ID cards/access cards that employees who work on several registers only need one card, as it is possible to code the card for the different access systems.

On Region Nordjylland's intranet there is also information on how to get access cards to the region's three hospitals, Aalborg University Hospital, Regionshospital Nordjylland and Psychiatry.

It appears from the procedure for Aalborg University Hospital that each department must appoint one or more authorized approvers who can order ID cards. This is a security measure so that not everyone can order ID cards.

It appears from the procedure for Regionshospital Nordjylland that the form for the ID card must be completed by the immediate manager.

As far as Psychiatry is concerned, the clinics and departments themselves choose how they want to organize the ordering of

ID cards, including whether it is the individual manager or a central person in the Clinic Management, the Secretariat or the Department Management who carries out the ordering of ID cards. An order form must also be completed when ordering an ID card.

It also appears from the procedure for issuing ID cards in Digitization and IT that ID cards must be ordered through the IT Secretariat, and that it is only when issuing ID cards to external employees that it is necessary to fill in a form for ID cards.

It appears from Region Nordjylland's procedures for access to data centers that only persons with a valid personal ID card may enter the data centers alone. The data centers are installed with scanners at the entrance, ensuring that only one person at a time can access the rooms. The person logs in with their access card and personal code.

Region North Jutland has stated that in relation to areas with computers with electronic patient records, the access restriction is not related to access cards. Access to the clinical systems requires a personal user for the region's IT systems. It is the employee's immediate manager and designated supervisors who assign access to and underlying access rights in the individual systems. This based on what is necessary to carry out the employee's work tasks.

The user can be used to log in to "terminals", desktop computers and laptops. The latter can be used from any location via VPN for a secure connection if it is from an external network. Similarly, you can log in via "ESA", Citrix desktop/session, which is also a secure connection. This happens with two-factor in the form of a unique SMS code if you log in from an external network.

Region North Jutland has also stated that the managers have a task every six months to ensure that their employees continue to have the necessary access – and the task is carried out continuously when there is a replacement.

In relation to the issuing of access cards, Region Nordjylland has stated that it is based on "authorised approvers", i.e. either immediate managers or trusted employees of these, approve that the individual employees are given access to the individual rooms. This applies to all rooms where an access card is required to gain access. This is based on an overall assessment that you as an employee should only have access to the rooms that are necessary for the solution of your work tasks.

Region Nordjylland has stated in this connection that an access card does not automatically grant access to all rooms on the land register on which you are employed, including e.g. all operating theaters and the like which contain external medical equipment such as MRI scanners or X-ray equipment. To gain access to these rooms, it must be selected for the individual employee's access card.

In conclusion, Region Nordjylland has stated that this is a practice that has been in place for a number of years, which is why a renewed and documented risk assessment in connection with GDPR has not been carried out.

4. The Danish Data Protection Authority's assessment

It follows from the data protection regulation, article 32, subsection 1, that the data controller must take appropriate technical and organizational measures to ensure a level of security appropriate to the risks involved in the data controller's processing of personal data.

The data controller thus has a duty to identify the risks that the data controller's processing poses to the data subjects and to ensure that appropriate security measures are introduced to protect the data subjects against these risks.

The Danish Data Protection Authority is of the opinion that the requirement for adequate security, cf. the data protection regulation, article 32, subsection 1, will normally mean that in premises where sensitive information, including health information, is processed, it must be ensured that unauthorized persons do not gain access.

After a review of the case, the Data Protection Authority finds that there is no basis for overriding Region Nordjylland's assessment that the procedures implemented for issuing access cards to the region's hospitals and premises in which personal data is processed constitute appropriate security measures, cf. Article 32 of the Data Protection Regulation.

The Danish Data Protection Authority has thereby emphasized that the North Jutland Region uses access control to locked rooms, that the region has procedures for issuing access cards, and that the region also has other security measures to prevent unauthorized persons from gaining access to personal data at the region's locations, e.g. requirements for a personal user for the region's IT systems and procedures for granting access to the systems.

—

[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] Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons in connection with the processing of personal data and on the free exchange of such information (the Data Protection Act).