Supervision of Region Central Jutland's issuing of access cards

Date: 01-12-2021

Decision

Public authorities

No criticism

Supervision / self-management case

Treatment safety

Access control

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

Journal number: 2021-422-0032

Summary

Region Central 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 Region Central Jutland'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 Central Jutland'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 Central Jutland Region uses access control to the region's premises where personal data is processed, that the region has procedures for issuing and withdrawing access cards, and that the region has other security measures to prevent unauthorized persons from gaining access to personal data on the region's locations.

Decision

1. Written supervision of Region Central Jutland's processing of personal data

Region Midtjylland 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 Central 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 Data Protection Authority notified the supervisory authority of the Central Jutland Region and, in this connection, requested an opinion, which the region issued on 2 July 2021.

On 14 September 2021, the Data Protection Authority requested a supplementary opinion, which Region Central Jutland issued on 5 October 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 Central Jutland'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 Central Jutland has stated that the region has a consolidated solution for electronic access control and production of access cards. The solution covers the majority of the region's hospitals, institutions (social area) and regional centers (administration) - however, with the exception of Hospitalsenheden Vest, which will only use the solution fully in connection with the move to Regionshospitalet Gødstrup.

Procedures for assigning and issuing access cards are documented in the region's electronic document management system for policies, guidelines and instructions. Region Central Jutland has forwarded guidelines prepared under the consolidated solution for Aarhus University Hospital, Regionshospitalet Randers, Regionspsychiatrien Randers, Hospitalsenheden Midt and Regionshospitalet Horsens. Allocating access cards to institutions and regional houses follows the procedures at the hospitals.

Several institutions in the social field have also drawn up additions to the consolidated solution.

Region Central Jutland has stated that the consolidated solution for access control consists of the following components:

X (excluded from publication):

all of the region's employees and associated externals are registered in X, so that the assigned user accesses are automatically activated and deactivated in line with hiring and terminations. In addition, employees can themselves maintain PIN codes for key cards in X self-service.

information to be used for key cards and access control is transferred […] to Y (exempted from publication). Among the information from X is information about what the employee's primary employment is. As a rule, only key cards are printed for the primary employment, even if employees has several jobs.

Y:

Y is used for the production of key cards and is installed locally on regionally approved PCs of the employees who handle card production.

In Y, a number of rules have been created which determine which Z (exempt from publication) systems an employee must be transferred to and which access groups the person must be enrolled in automatically.

Y has interfaces for the approved Z systems and transfers relevant information in the following situations:

when a new card is printed

when a card is retransferred manually

when there are updates to master data from X (e.g. a new end date or organizational association of employees).

The Z systems:

In the consolidated solution, four Z systems have been approved.

Y transfers information about master data, automatically assigned rights and card information.

In addition to the automatically assigned access, the operators in the individual Z systems can assign rights manually to individual persons/groups. This takes place on the basis of management approval.

It generally appears from the forwarded guidelines on the allocation and issuing of access cards that all employees must carry an ID/access card when they are at work.

By default, the access card will either be coded to […]. If an employee needs access to other rooms, the employee must contact his manager. Upon termination of employment, the card must be handed in to the immediate manager.

It also generally appears from the guidelines that the use of ID/access cards is logged automatically.

Region Midtjylland has stated that, in principle, the region has open hospitals, which is why certain areas are open to the public. Areas below, where personal data is processed, are staffed by the region's employees who are instructed in information security.

[…]

It appears from Region Central Jutland's information security handbook that systems for access control are an element of physical security that ensures that only persons with a legal mission gain access to the region's area.

Safe areas […]. Access to secured areas must be locked and monitored. […]

Craftsmen, repairmen, technicians and other professional groups must, to the extent necessary, be given work-related access to Region Central Jutland's IT resources. Access must be documented and be time-limited. Any exemption can be granted by the region's IT security manager.

It also appears from the information security handbook that information about secure areas and their function must only be given based on a work-related need. Special attention is drawn to offices and other premises where personal data or confidential information is stored. […]

Access to server rooms and main intersections is only permitted with security approval or with supervised access by employees from the IT department.

It is Region Central Jutland's view that the forwarded guidelines are an expression of the region's risk considerations for managing and granting access rights. Access to locations where personal data is processed is granted on the basis of risk considerations, meaning that access is only granted to employees who are employed for the purposes for which the specific personal data is processed or employees who, based on operational or system technical considerations, have a valid need for access.

Region Central Jutland has stated that the region is aware that the behavior of employees can pose a particular risk if the guidelines are not observed - both in managing and granting access and in relation to physical security in general. In order to limit this risk, the region constantly focuses on continuously informing employees about correct behavior in relation to physical security.

In this connection, Region Central Jutland has referred to the information security handbook, according to which employees are instructed to always log off PCs and other electronic equipment when they are left. The equipment is always protected by username and password regardless of physical location. Furthermore, there is no data locally on the region's PCs. All PCs are also installed with automatic log off after a certain period of time.

It appears from Region Central Jutland's guidelines and guidance for employees on setting up and using large screens for clinical logistics that, as a general rule, no sensitive data may appear on the screens that are not necessary for the performance of tasks, and the information may not be shown to unauthorized persons.

Region Central Jutland has stated that the region continuously prioritizes carrying out awareness activities. The region has referred to a more recent awareness campaign, where employees were made aware of essential elements related to physical security through e.g. the themes "screen off unauthorized persons" and "help guests well on their way", which illustrate risk considerations in relation to the fact that there are many people in the region's locations - both employees and patients. Region Central Jutland has also stated that the themes address the importance of ensuring that unauthorized persons do not go places where they should not and/or are given the opportunity to view personal data without authorization.

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 Central Jutland'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 hereby emphasized that the Central Jutland Region uses access control to the region's premises where personal data is processed, that the region has procedures for issuing and withdrawing access cards, and that the region also has other security measures to prevent unauthorized persons from gaining access to personal data on the region's locations, e.g. password on the region's PCs, guidelines for using screens and awareness courses.

[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 data protection regulation).[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 (Data Protection Act).