The region of Southern Denmark is recommended for a fine

Date: 16-07-2021

Decision

Public authorities

Police report

Reported breach of personal data security

Treatment safety

Access control

Children

Sensitive information

Unauthorized access

The Danish Data Protection Authority reports the Region of Southern Denmark to the police, as the Danish Data Protection Authority assesses that the region has not met the requirements for an appropriate level of security in the data protection regulation.

Region South Denmark has been fined DKK 500,000 for not having complied with its obligation as data controller to implement appropriate security measures. The Danish Data Protection Authority became aware of the case when a citizen contacted the Danish Data Protection Authority in 2020 about a lack of security in the region's processing of personal data relating to the citizen's child, and shortly afterwards the region reported the matter as a breach of personal data security to the Danish Data Protection Authority.

For a period of more than 1.5 years, the Region of Southern Denmark had had a database for research and clinical purposes, where the region had not sufficiently safeguarded against unauthorized access to PDF documents in the database by simply changing a URL address. This meant that citizens who were registered in the database - and who also had a login to the database - could access personal data about the more than 30,000 others registered in the database. In the database there were, among other things, questionnaires containing health information on more than 30,000 children associated with psychiatry.

The vulnerability in access to the database does not appear to have been exploited by anyone other than the citizen in

question who became aware of the situation. This is supported by the region's log, which shows that the information has not been accessed by other unauthorized parties.

Requirements for adequate security

It is the opinion of the Danish Data Protection Authority that handling of e.g. health information about a particularly vulnerable group of minors places greater demands on the authority's care in connection with the processing of personal data. A processing activity where personal data is stored in a database and passed on via a URL solution must take place in a way that ensures the necessary confidentiality, so that there is no potential access to personal data worthy of protection.

"As a public authority, you have a special responsibility to take good care of citizens' information. In a situation like this, there is a vulnerability that has been easy to identify. With relatively basic IT knowledge, you can see from the URL that it can be changed so that you can potentially access other documents. This means that there is a greater risk of the access being misused. In addition, it is a well-known vulnerability that should have been taken into account during the development of the solution, and which should at least have been discovered in connection with testing," explains Frederik Viksøe Siegumfeldt, head of office at the Data Protection Authority.

Why report to the police?

The Danish Data Protection Authority always makes a concrete assessment of the seriousness of the case pursuant to Article 83, paragraph 1 of the Data Protection Regulation. 2, when assessing which sanction is the correct one in the opinion of the supervisory authority.

When assessing that a fine should be imposed, the Danish Data Protection Authority has emphasized that it is health information about a vulnerable group of children. Furthermore, there is a lack of development and regular testing, assessment and evaluation of the effectiveness of a previously known incident and vulnerability - as the region has previously reported a similar breach of personal data security to the Norwegian Data Protection Authority, which gave rise to serious criticism from the authority.