Police report

SIRIUS lawyers are recommended for fines

Date: 14-07-2022

Decision

Private companies

Police report

Reported breach of personal data security

Treatment safety

Hacking and others

Unauthorized access

Particularly sensitive personal data was compromised when SIRIUS lawyers were exposed to a hacker attack. Due to a lack of security measures, the Danish Data Protection Authority reported the company to the police and recommended a fine of DKK 500,000.

SIRIUS lawyers have been fined DKK 500,000 for not having implemented basic security measures when setting up remote access to the company's IT systems with personal data of a particularly protective nature.

In March 2020, SIRIUS lawyers reported a breach of personal data security to the Norwegian Data Protection Authority after they were exposed to a hacker attack. In the attack, hackers gained access to and encrypted the law firm's servers, which contained information about the company's clients and counterparties. This created a serious risk of the information about the persons falling into unauthorized hands, with potential damage to the persons concerned as a result.

Lack of basic safety measures

"Law firms naturally process a lot of information that requires special protection. In this case, SIRIUS lawyers lacked basic security measures, and this unfortunately meant that, among other things, clients' information was compromised. You cannot protect yourself 100% against hacker attacks, but the rules in the GDPR require that you make an effort to avoid what corresponds to the risk," says Betty Husted, deputy in the Data Protection Authority.

In systems with a large number of personal data of a particularly protective nature, where compromise would entail a high risk for the rights of the data subjects, the data controller must have specially qualified security measures to ensure that

unauthorized access to personal data does not occur.

When you create remote access to such IT systems, you must therefore have implemented measures for verification, such as multifactor login.

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.

In assessing that a fine should be imposed, the Danish Data Protection Authority emphasized that SIRIUS lawyers had not implemented the security measures that are expected as a minimum when using remote access to systems that, if compromised, would entail a high risk for the data subject's rights.

In its proposal for the size of the fine, the Danish Data Protection Authority has, among other things, emphasized the nature and seriousness of the infringement and the regulation's requirement that a fine in each individual case must be effective, proportionate to the infringement and have a deterrent effect.

Furthermore, it has been concluded, among other things, that SIRIUS lawyers were in the process of implementing a multi-factor authentication solution at the time of the breach. At the same time, the Danish Data Protection Authority has emphasized that SIRIUS lawyers have acted extremely cooperatively in relation to the disclosure of the case.

Read more

You can read more about security here.