Police report

Lolland Municipality is recommended for a fine

Date: 11-08-2022

Decision

Public authorities

Police report

Reported breach of personal data security

Treatment safety

Social Security number

Sensitive information

Unauthorized access

Citizens' information was exposed to an unnecessary risk, as Lolland Municipality's employees were able to disable access codes on phones and tablets. The Danish Data Protection Authority has reported the municipality to the police and recommended a fine of DKK 50,000.

Lolland Municipality has been fined DKK 50,000 for not having implemented basic security measures in the form of unavoidable requirements for access codes on the municipality's mobile devices.

"Municipalities process large amounts of sensitive information about citizens, and therefore they also have a responsibility to look after this information properly. Mobile devices are occasionally stolen, forgotten or lost, and if unauthorized persons can easily access the information on them, then you are not living up to that responsibility," says Betty Husted, deputy in the Danish Data Protection Authority.

The Danish Data Protection Authority became aware of the situation through a notification from Lolland Municipality in December 2020, when an employee in the municipality had a work phone stolen. Via the phone, there was access to the employee's work email account, which contained information about several citizens' names, social security numbers, health information and abuse.

The phone was not protected by a code as it was switched off. Therefore, there was access to the information that was on the phone. The municipality stated that over a number of years it had been possible for employees to remove the otherwise

mandatory access codes, so that telephones could be used without the use of a code. The municipality had immediately initiated restorative measures in the form of new precautions and changes in the technical set-up of telephones handed out.

Lack of technical measures

The Norwegian Data Protection Authority finds that Lolland Municipality's processing of personal data was not in accordance with the rules on adequate security.

In the assessment, the Danish Data Protection Authority has, among other things, emphasized that a data controller must assume that not all employees at all times follow internal guidelines that mobile devices must always be protected by a password. Really effective protection is thus dependent on such a password not being bypassed, e.g. in that the individual user can switch off the code.

It is also the Danish Data Protection Authority's assessment that stolen mobile devices are generally examined for personal data to a greater extent than previously, such as e.g. credit card information and social security numbers before these are disposed of, e.g. on resale.

Considering the risks for citizens linked to Lolland Municipality's processing of personal data, the Danish Data Protection Authority is of the opinion that it is unjustifiable that the municipality had not protected its mobile devices with a password that the employees could not turn off themselves.

Why report to the police?

The Danish Data Protection Authority always makes a concrete assessment of the case in accordance with the regulation's article 83, subsection 2, when assessing which response is, in the opinion of the supervisory authority, the most appropriate.

In making the recommendation to the police, the Data Protection Authority has, among other things, emphasis has been placed on the fact that this is a public authority which generally has a special responsibility for protecting citizens' information, and that Lolland Municipality processes large amounts of confidential and sensitive information in that capacity, and that, in the opinion of the inspectorate, there is a lack of implementation of a general and basic technical measure.