

The Danish Immigration Service is recommended for a fine

Date: 17-08-2021

News

The Danish Data Protection Authority reports the Danish Immigration Service to the police, and recommends a fine of DKK 150,000, as the Danish Data Protection Authority assesses that the agency has not met the requirements for an appropriate level of security in the data protection regulation.

On 25 August 2020, the Danish Data Protection Authority initiated a case of its own initiative against the Ministry of Immigration and Integration, when the Danish Data Protection Authority became aware through media coverage that a possible logging error in an IT system associated with the Departure Center Kærshovedgård could have had consequences for the residents' rights and freedoms.

After an investigation into the case, it became clear that the Immigration Service was responsible for the processing of personal data in connection with checking the residents' residence and notification obligations at the Departure Center Kærshovedgård and the Departure Center Sjælsmark.

In the spring and summer of 2020, a number of security incidents occurred regarding lack of registrations in the system, which registers that residents at Udrejsecenter Kærshovedgård and Udrejsecenter Sjælsmark comply with their residence, notification and reporting obligations. The lack of registrations led to the initiation of proceedings regarding the reduction of a number of residents' cash benefits as well as the police reporting of a number of residents for non-compliance with the rules in the Aliens Act.

Violation of the rules of adequate security

After a review of the case, the Danish Data Protection Authority finds that the Danish Immigration Service's processing of personal data has not been in accordance with the rules on appropriate security.

In assessing this, the Norwegian Data Protection Authority has emphasized that the Danish Immigration Service had not introduced procedures to systematically use the information in the incident log, which records the movements of the residents inside the Departure Center Kærshovedgård. This also applies at Udrejsecenter Sjælsmark to the extent that it could contribute to checking the correctness of registrations of residents' movements - in connection with the processing of notification cases as part of the control of residence and notification obligations.

In addition, the Danish Data Protection Authority has emphasized in the assessment that the Danish Immigration Service had not identified and dealt with risks for the data subjects in connection with the processing activities in the SALTO system. Finally, the Danish Data Protection Authority has emphasized that the Danish Immigration Service – in view of the legal consequences for the residents associated with the registrations in question – had not made sufficient backups of the information that is processed in the SALTO system. It was therefore not possible for the agency to recreate a number of the data that was lost during the incident on 9-10 June 2020.

The Danish Data Protection Authority is of the opinion that with information and registrations that form part of the chain of criminal proceedings or are used for control measures that are subject to sanctions, it must be ensured that all activities are logged and that a backup copy is made at such intervals that data is not lost in case of breakdown. In addition, it is the opinion of the supervisory authority that a backup procedure must be checked with a disaster recovery test at intervals determined according to the risk to the rights of the data subjects.

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.

"We take this case very seriously because it is about the fundamental right that one should be able to trust the information that the authorities process and pass on to the police, and which may ultimately end up as evidence in court. It is very important that such information is correct. In addition to the loss of rights for the people it concerns, a lack of data protection in the chain of criminal proceedings also leads to weakened trust in both the authorities and the courts", explains head of office in the Data Protection Authority Frederik Siegumfeldt.