

Examination of selected safety areas: Slagelse Municipality

Date: 15-01-2021

Decision

Public authorities

Based on Slagelse Municipality's answers to the submitted questions, the Danish Data Protection Agency's overall assessment is that Slagelse Municipality's general maturity in the area of security is an expression of a level that matches the risks that the organization's processing activities pose to the data subjects' rights and freedoms.

Journal number: 2020-423-0232

Summary

As part of the Danish Data Protection Agency's work to strengthen the data and risk-based approach to guidance and control, the Authority completed a number of questionnaire surveys in December 2020. The surveys were intended to shed light on the general maturity of selected security areas at seven public authorities and seven private companies. The questionnaires included i.a. issues for handling backup and breaches of personal data security as well as preparation of information security policies, contingency plans and documentation.

The Danish Data Protection Agency can state that the handling of backup in particular is an area that has the attention of the data controllers. In several cases, however, the Danish Data Protection Agency has assessed that the data controllers may have a greater focus on the establishment of contingency plans and contingency plans.

On 10 July 2020, the Danish Data Protection Agency sent a questionnaire to Slagelse Municipality.

The Data Inspectorate's purpose in conducting the written questionnaire survey was in particular to make an assessment of Slagelse Municipality's maturity in the area of data protection with a special focus on handling breaches of personal data security and compliance with information security requirements, including handling documentation, backup and contingency plans.

The Danish Data Protection Agency has also, on the basis of Slagelse Municipality's response, made an overall assessment of the measures that Slagelse Municipality has assessed as appropriate to address risks that the organization's processing activities pose to the data subjects.

1. The Danish Data Protection Agency's assessment

1.1. Established security measures

Article 32 (1) of the Data Protection Regulation [1] 1, states, inter alia, that the data controller, taking into account the current technical level, the implementation costs and the nature, scope, coherence and purpose of the treatment in question, as well as the risks of varying probability and seriousness for natural persons' rights and freedoms, implement appropriate technical and organizational measures to ensure a level of safety appropriate to these risks.

Based on Slagelse Municipality's answers to the submitted questions, the Danish Data Protection Agency's overall assessment is that Slagelse Municipality's general maturity in the area of security is an expression of a level that matches the risks that the organization's processing activities pose to the data subjects' rights and freedoms.

In this connection, the Danish Data Protection Agency's assessment is that in particular Slagelse Municipality's responses regarding information security policies and handling of security breaches are an indication that the organization has actively addressed any risks to the data subjects, that the organization has established procedures and guidelines for security. and that the organization has otherwise established relevant and appropriate security measures.

With regard to risk assessment, backup and contingency plans, however, the Danish Data Protection Agency has noted that Slagelse Municipality has stated that in certain areas only partially implemented planned measures have taken place. Overall, however, the Danish Data Protection Agency finds that Slagelse Municipality's responses leave an impression that the organization is actively working on this, and on that basis the Authority finds no basis for taking further action on that occasion.

1.2. Especially about documentation

Article 5 (1) of the Data Protection Regulation 2, states that the data controller is responsible for and must be able to demonstrate that the data controller complies with the principles for the processing of personal data mentioned in Article 5, para. 1, including i.a. personal data is processed in a way that ensures adequate security for the personal data in question, in accordance with Article 5 (2). 1, letter f.

In continuation of the above, however, the Danish Data Protection Agency has noted that Slagelse Municipality, according to the information, has only to a varying extent prepared documentation in relation to backup and contingency plans. On the basis of the answers given, it is therefore the Authority's immediate assessment that Slagelse Municipality may, depending on the circumstances, have difficulty - within a reasonable time - demonstrating (documenting) that personal data is processed in all cases in a way that ensures adequate security for the personal data in question, in accordance with Article 5 (1) of the Data

Protection Regulation. Article 5 (2) 1, letter f.

Based on Slagelse Municipality's answers in relation to documentation, the Danish Data Protection Agency finds that there are circumstances which indicate that Slagelse Municipality can advantageously increase its focus on providing the necessary documentation, if this has not already happened. Overall, however, the audit finds that Slagelse Municipality's responses leave an impression that the organization has such maturity and works with data protection in such a way that there is no basis for the audit to take further action on that occasion.

The Danish Data Protection Agency considers the case closed and will not take any further action.

The Danish Data Protection Agency's opinion can be brought before the courts, cf. section 63 of the Constitution.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).