Examination of selected security areas: IT University (ITU)

Date: 15-01-2021

Decision

Public authorities

Based on the ITU's answer to the submitted questions, the Data Inspectorate's overall assessment is that the ITU's general maturity in the field of security is an expression of a level that corresponds to the risks that the organization's processing activities pose to the data subjects' rights and freedoms.

Journal number: 2020-41-0065

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 the IT University of Copenhagen (ITU).

The purpose of the Danish Data Protection Agency's conduct of the written questionnaire survey was in particular to make an assessment of ITU's maturity in the field 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 the ITU's response, made an overall assessment of the measures that the ITU has assessed as appropriate to address the 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 the ITU's answer to the submitted questions, the Data Inspectorate's overall assessment is that the ITU's general maturity in the field of security is an expression of a level that corresponds to 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 ITU's responses regarding information security policies, 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.

However, with regard to updating the list as well as handling backup and contingency plans, the Danish Data Protection Agency has noted that the ITU has stated that in certain areas only partially implemented planned measures have taken place. Overall, however, the Danish Data Protection Agency finds that ITU's responses leave the impression that the organization is actively working with these areas, including continued implementation, and on that basis the Authority finds no basis for 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. that personal data is processed in a way that ensures adequate security for the personal data in question, in accordance with Article 5 (1); 1, letter f.

In relation to individual issues, the ITU has stated that no documentation has been prepared. For the majority of ITU's responses, however, it appears that there is documentation in a structured and management-approved form. However, with regard to the submission of this documentation, the Authority is committed to the fact that the ITU will only be able to submit the documentation with a 4-week deadline.

In this connection, the Danish Data Protection Agency must draw attention to the fact that this type of documentation - after the

Authority's immediate assessment - must be able to form the basis for ITU's internal work to maintain an appropriate level of security, including the university's compliance with data protection requirements. it may be necessary that the documentation is easily accessible to relevant parts of the organization.

Overall, the Danish Data Protection Agency finds that the ITU's responses leave the impression that the university is not able to provide the necessary documentation within an appropriate period of time, and that there are circumstances which indicate that the ITU can advantageously increase its focus on prepared documentation is to a greater extent made easily accessible to relevant employees, etc.

Furthermore, on the basis of the answers given, it is the Authority's immediate assessment that the ITU may have difficulty in - within a reasonable time - demonstrating (documenting) that personal data is in all cases processed in a way that ensures adequate security for the persons concerned. personal data in accordance with Article 5 (1) of the Data Protection Regulation Article 5 (2) 1, letter f.

On the present basis - including an overall assessment of the ITU's responses - the Danish Data Protection Agency will not take any 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).