The Danish Health Data Agency is criticized for a lack of control over personal data in the IT environment

Date: 16-03-2022

Decision

Public authorities

Criticism

Reported breach of personal data security

Treatment safety

Sensitive information

The Danish Data Protection Authority expresses criticism in a new decision, which emphasizes that a data controller must check whether personal data has been stored in IT environments by mistake, regardless of whether the IT environments may not be used for storing personal data.

Journal number: 2021-442-12991

Summary

The Norwegian Data Protection Authority has made a decision in a case where an employee at the Danish Health Data Agency, in violation of internal guidelines and procedures, had saved a data set - containing pseudonymised personal data - in the Microsoft Azure DevOps development environment, where they were not allowed to be saved. The data set contained pseudonymised confidential information about citizens, which could be "decoded" by trusted employees, regardless of whether they had a work-related need for it.

The Danish Health Data Agency only discovered a year later that the data set had been stored in the IT environment used for task management. The Danish Health Data Agency informed the Danish Data Protection Authority that data sets that are stored in the IT environment are generally not checked for personal data and that it is not possible to establish technical security measures to ensure that a similar human error does not occur in the future.

The Danish Data Protection Authority found that the Danish Health Data Agency – by not having established appropriate controls to ensure that there was no personal data in the system – had not complied with the rules on processing security.

The Danish Data Protection Authority emphasized that data controllers must generally establish controls – either manual or automatic – to ensure that personal data is not stored in IT environments where it is not allowed to be. In this connection, it is

not sufficient to have guidelines and procedures for whether information may be stored in an IT environment, without regularly checking whether they are followed in practice. The Danish Data Protection Authority also emphasized that it was a so-called "agile development environment", where there is a known risk of personal data being stored by mistake.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there is a basis for expressing criticism that the Danish Health Data Agency's processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 32, subsection 1.

Below follows a closer review of the case and a rationale for the Data Protection Authority's decision.

2. Case presentation

On 12 May 2021, the Danish Health Data Protection Agency reported a breach of personal data security to the Norwegian Data Protection Authority.

The Danish Data Protection Authority subsequently sent a hearing to the Danish Health Data Agency on 22 June 2021, to which the Danish Health Data Agency responded on 8 July 2021.

It then appears from the case that a former employee, in connection with the internal sharing of a data extract, in violation of the Danish Health and Data Protection Agency's internal guidelines and procedures, saved the data extract, which, among other things, contained pseudonymised health information about citizens in the Capital Region, in Microsoft Azure DevOps, where the data extract was stored for a period from June 2020 to May 2021. In this connection, the Danish Health Data Agency has stated that both internal and external consultants are instructed in applicable procedures, which appear from the agency's development handbook, which i.a. describes which information must be stored in DevOps, including that no personal data must be stored - apart from names of case handlers etc. in connection with task management – in DevOps.

It also appears from the case that the data set, which the employee saved in DevOps, originates from the Hospital Medicines Register and contains information on gender, age, municipality, region and prescribed/administered medicine of registered persons from the Capital Region for the period between May 2018 and January 2020 and spans 877,813 drug administrations.

In this connection, the Danish Health Data Agency has clarified that personal numbers included in the data set in the Hospital Medicines Register are replaced by "xxx" when extracting, which is why the data set is pseudonymised when the information is processed by employees of the Danish Health Data Agency. In this connection, the Danish Health Data Agency has stated that

several internal and external employees in the agency, by virtue of their position and associated tasks, have access to personally identifiable information in the Hospital Medicine Register, which is why it is possible for these persons to identify the personal data that appears in the specific data set.

The Danish Health Data Agency has finally stated that the data set was protected by the agency's own domain DKSUND, which is located in Azure Active Directory. DevOps is used i.a. by several departments in the Danish Health Data Agency for task management, and it requires authorization and authentication to access the service. The Danish Health Data Agency has further stated that every data set stored in DevOps is not checked and that it is not possible to establish technical measures that can counter the fact that a similar human error results in a breach of personal data security, e.g. . in that certain file formats cannot be uploaded in DevOps.

3. Reason for the Data Protection Authority's decision

3.1. Article 32 of the Data Protection Regulation

It follows, among other things, of the data protection regulation, article 32, subsection 1, that the data controller, taking into account the current technical level, the implementation costs and the nature, scope, context and purpose of the processing in question, as well as the risks of varying probability and seriousness to the rights and freedoms of natural persons, implements appropriate technical and organizational measures to ensure a level of security, appropriate to these risks.

It also follows from Article 32, subsection 1, letters b and d, that the data controller in that connection – and depending on what is relevant – i.a. must implement measures to maintain an ability to ensure ongoing confidentiality, integrity, availability and robustness of processing systems and services, as well as procedures for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure processing security.

In this connection, the Danish Data Protection Authority is of the opinion that the data controller must deal with the risk that personal data is stored in an environment (even by mistake), regardless of whether the environment is intended for the storage of personal data. In continuation of this, it is the authority's assessment that guidelines regarding the storage and deletion of personal data in a given system or area cannot justify not checking whether information is stored in the system or area - especially in situations where agile development environments such as DevOps. In connection with this, the Danish Data Protection Authority is of the opinion that there is – especially where uploading is not controlled – a known risk of personal data being stored by mistake in agile development environments, which emphasizes the need for the environments to be regularly

checked for whether information is inadvertently stored in the environment.

On this basis, the Danish Data Protection Authority finds that the Danish Health and Data Protection Agency - does not sufficiently control whether personal data is inadvertently stored in environments which, in the specific case, e.g. may lead to personal data being made available to unauthorized persons - had not established a security level that suited the risks posed by the agency's processing of personal data, cf. Article 32, subsection 1.

The Norwegian Data Protection Authority has placed emphasis on the fact that the Danish Health Data Agency has not established appropriate organizational or technical security measures to ensure that no personal data is stored in the DevOps environment, including e.g. regular technical review – such as scanning of the environment – or by manual control.

Furthermore, the Danish Data Protection Authority has emphasized that the incident includes special categories of personal data about a large number of citizens, and that the incident lasted approx. one year.

In a mitigating way, the Danish Data Protection Authority emphasized that the personal data had been pseudonymised and that the information had only been made available to trusted employees.

In summary, the Danish Data Protection Authority finds that there is a basis for expressing criticism that the Danish Health and Data Protection Agency's processing of personal data has not taken place in accordance with the rules in the Data Protection Regulation, Article 32, subsection 1.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data and on the repeal of Directive 95/46/EC (general regulation on data protection).