Summary Final Decision Art 60

Complaint

Violation identified, Administrative fine.

EDPBI:FI:OSS:D:2022:604

Background information

Date of complaint:	26 October 2020
Draft decision:	10 November 2022
Revised draft decision:	N/A
Date of final decision:	09 December 2022
Date of broadcast:	15 December 2022
Controller:	[redacted]
Processor:	N/A
LSA:	FI
CSAs:	EE, NO, SE
Legal Reference(s):	Article 5 (Principles relating to processing of personal data), Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 13 (Information to be provided where personal data are collected from the data subject), Article 15 (Right to access by the data subject). Article 25 (Data protection by design and by default)
Decision:	Violation identified, Administrative fine.
Key words:	Health records, Accuracy, Right of access, Data subject rights, Transparency, Data protection by design and by default, Administrative fine.

Summary of the Decision

Origin of the case

On 26 October 2020, the complainant lodged a complaint with the LSA. The complainant alleged that the controller had maintained an extensive data file containing health information on its employees, this data file included the times of absence due to illness and the employees' diagnoses. The data of the complainant was stored in this file for 20 years and the data in the file was also partly inaccurate. Furthermore, the complainant alleged that this data was used against her when she contested her dismissal. She has asked the controller for access to her personal data and said that she has requested

access to the log data related to the data file in question. The complainant has not been given access to the log data. Information on the diagnose listing included in the data file had not been given to the complainant. The information provided by the controller confirmed that it had maintained two data files intended for internal use (the MAPS human resources management system and Medakt patient record system), which had contained employees' health information, among other things. The controller had processed employees' health information for the payment of sick pay or comparable benefits linked to the employee's health. When an employee had fallen ill while working on a ship, the ship's nurse had recorded this in the Medakt patient record system. If the illness led to sick leave, this was recorded in the MAPS system after the employee had delivered the sick leave certificate. Health information had only been processed by the employees of the controller tasked with preparing, making or implementing employment-related decisions based on such information. At the moment of the decision of the LSA, the data in the Medakt system had been stored for an indefinite period. Data subjects had the right to review data saved in the MAPS and Medakt systems. The data had also been updated, when necessary. According to the information provided by the controller, the information on the complainant's sick leave certificates was given to the complainant insofar as it was available. The oldest information had already been erased.

Findings

The LSA found that the controller: had not complied with the provisions of the Working Life Privacy Act when saving diagnoses into the MAPS system; had not complied with the provisions of the Working Life Privacy Act when storing its employees' health information in the MAPS system; had not taken every reasonable step under Article 5(1)(d) and Article 25(1) of the GDPR in order to ensure that the personal data processed in the MAPS system was accurate and up to date; had not complied with the provisions of Article 5(1)(a) and Article 13 of the GDPR; had not complied with the provisions of Article 12(3) of the GDPR when replying to the complainant's request made pursuant to Article 15 of the GDPR; had not complied with the provisions of Article 15(1) of the GDPR when replying to the complainant's request made pursuant to Article 15 of the GDPR. The LSA found that the employer nevertheless had the right to process, for example in its HR systems, data concerning the dates and lengths of an employee's absence from work due to sick leave. However, information on the causes of the absence due to illness, such as the disease or injury or its nature or diagnosis, may not be saved into HR systems. The medical certificates or statements delivered to the employer by the employee must be stored separately from other personal data concerning the employee. The LSA found that the controller had not presented any grounds by virtue of which the complainant's data could have been stored for 20 years in the MAPS system nor any justification for retaining the health information of its employees in the MAPS system for ten years from the end of the absence. The LSA found that the controller had not taken every reasonable step under Article 5(1)(d) and Article 25(1) of the GDPR to ensure the accuracy of the personal data processed in the MAPS system. The Deputy Data Protection Ombudsman thus finds that the controller had not complied with the provisions Article 5(1)(a) and Article 13 of the GDPR. Since information on the complainant's diagnoses was later disclosed to the police, the LSA found that the basis for the disclosure may be assessed as a criminal matter. The complainant may turn to the police on this matter.

Decision

The LSA issued a reprimand to the controller under Article 58(2)(b) of the GDPR. The controller had not complied with the following provisions referred to in Article 83(5) of the GDPR: 1) Article 5(1), points (d) and (a); 2) Article 13; 3) Article 12 (3); 4) Article 15(1) And 5) 25(1) of the GDPR. The LSA found an administrative fine of EUR 230,000 to be effective, proportionate and dissuasive.