GDPR Case Study: Can Employers Access Both the Work-Related and Non-Work-Related Private Data of Their Former Employees?

Victor Mora
Brown University

Abstract

An unnamed public sector employer was accused of not giving prior notice to a former employee that his archived emails were being restored with the intent to search for a work-related document. Without prior notice, the ex-employee was unable to first go through and delete private information including passwords and personal financial data that were also present in his old work email. The employer was found guilty, and the Hungarian National Authority for Data Protection and Freedom of Information (Hungarian: Nemzeti Adatvédelmi és Információszabadság Hatóság, henceforth referred to as the NAIH) issued a fine of 1500 EUR. The NAIH found that the contents of the business email account constituted private data belonging to the employee. Furthermore, the NAIH directed the employer to implement internal policies to protect personal data, as well as give adequate notice to employees in the future. It dictated that there must be a legal basis to process private emails, even in archived form.

1. Introduction

On July 27, 2018, an application was submitted to the NAIH by a former director of a hospital. The applicant alleged that the former employer had reinstated his email account a year after he left and parsed its contents looking for business documents after his legal separation from the company. This action could have inadvertently exposed private information stored in the email account, including the former employee's private data such as passwords and financial information. [1] The applicant found out that this had transpired from an ex-coworker that was still under employment with the hospital. When the applicant called current leadership, it was confirmed that his emails had been searched without his prior notice. The ex-employee felt as though his right to fair data processing was violated, given that the archived email account had private data, the ex-employee was not informed of his former employer's access to the contents of the mailbox, and the ex-employee was not able to be present when his former employer searched the archived mailbox. [2]

In this case, the applicant (former employee) is the data subject, whose sensitive data was stored by the hospital (former employer), who was the data controller. The role of data processor was also performed by the former employer, as the hospital was in charge of both maintaining the archived email accounts and parsing them for their own purposes. As the data protection agency for the case, the NAIH determined that a number of articles of the GDPR had been violated, mostly pertaining to not complying with general data processing principles. [3]

2. GDPR Violations

The NAIH found that the former employer's actions were a breach of a number of Articles of the GDPR, in particular Articles 5, 6, 13, 24, and 25. [3]

2.1. Article 5: Principles relating to processing of personal data

Article 5 of the GDPR states that:

"1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject...

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed… ('storage limitation');

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')." [6]

It was found that the former employer's processing of the data was not transparent with regards to point a. of subparagraph 1, as the former employee was not notified of the processing nor able to be present during the processing. With regards to point e, the period over which the ex-employee was identifiable by the data was longer than necessary due to the presence of personally identifiable personal data in the archived emails. Thus, the former employer was unable to demonstrate compliance under subparagraph 2. The former employer could have remained in compliance by notifying the ex-employee, allowing him time to remove his personal data from the archived account, and allowing him to be present during the parsing of the email account content.

2.2. Article 6: Lawfulness of processing

Article 6 of the GDPR states that:

"1. Processing shall be lawful only if and to the extent that at least one of the following applies:" [6], followed by a set

of circumstances in which processing is lawful. The NAIH found that the employer's basis was "not sufficient to support the lawfulness of data processing" [5] (translated from Hungarian to English). The former employer might have been able to stay in compliance by following the same set of steps outlined in section 2.2.

2.3. Article 13: Information to be provided where personal data are collected from the data subject

Article 13 of the GDPR states that:

2. ...the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;" [6]

As the ex-employee did not have any knowledge that the personal data would be archived and not deleted upon his exit from employment, and was not aware of his right to rectify or delete his personal information from the email account, the former employer was in violation of subparagraph 2 of Article 13 of the GDPR. This could have been prevented if the employer had notified employees of precisely how their email accounts would be handled if they left the company (archived, not deleted), and that the employees had a right to rectify or delete their personal, identifiable, or sensitive data from the archive, especially since that data was not relevant to the business documents or proceedings that were also present in the archive.

2.4. Article 24: Responsibility of the controller

Article 24 of the GDPR states that:

"1. ...the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller." [6]

It was determined by the NAIH that the employer " ha[d] not taken the necessary appropriate technical and organizational measures" [5] as described by Article 24 of the GDPR. Indeed, in their decision the NAIH laid out that "employers must adopt internal policies on archiving and the use of IT assets and e-mail accounts" [3], which would constitute appropriate measures.

2.5. Article 25: Data protection by design and by default

Article 25 of the GDPR states that:

1. ...the controller shall...implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons." [6]

Similar to Article 24, Article 25 contains measures that should be adopted by employers as an internal policy, which the hospital in this case lacked. By implementing the same measures discussed in section 2.4, the former employer would be able to remain in compliance with regards to Article 25.

3. Discussion

Evaluating the case, it appears that the cause of the violations was not technical in nature. The true question seems to be, "could the data controller be allowed to process non-work and work related personal data of the former employee in any situation?". [4] The NAIH seems to have decided that employees and ex-employees have protections when it comes to their private information stored in company accounts. As the company made a number of missteps that led to the documented violations, the violations could have been prevented by (1.) encrypting the data/email account so as to prevent people without the appropriate access (including at the company) from accessing the sensitive information, and (2.) having a notification process in place for former employees, so that they have a chance to delete their sensitive information before their former employer goes looking through their old email accounts for business related information.

In terms of the fine, a cost of 1500 EUR does not seem like a significant amount. However, the real deterrent and motivator toward establishment of organizational measures

recommended by the NAIH comes from the prospect of repeated fines from the complaints of subsequent ex-employees. Violations like the one in this case are likely commonplace, not just for this employer but others as well without an up-to-date archival protocol or privacy policy. Other companies that are organizationally similar to this employer might do well to heed the warning that this case provides them.

References

[1] CMS Law-Now Data authority issues two fines for unlawful access to workplace emails https://www.cms-lawnow.com/ealerts/2020/01/data-authority-issues-two-fines-for-lawful-access-to-workplace-emails?cc_lang=en, January 2020. (Accessed on 09/24/2021).

[2] Lexology.com Dániel Gera. Access to Employee Emails – Enhanced Authority Control https://www.lexology.com/commentary/employment-immigration/hungary/schoenherr/access-to-employee-emails-enhanced-authority-control, August 2020. (Accessed on 9/24/2021).

[3] enforcementtracker.com ETid-157

[4] gdprhub.com NAIH - NAIH/2019/51/11 https://gdprhub.eu/index.php?title=NAIH_-_NAIH/2019/51/11, December 2019. (Accessed on 9/24/2021).

[5] Nemzeti Adatvédelmi és Információszabadság Hatóság Case number: NAIH / 2019/51/11 https://www.naih.hu/files/NAIH-2019-51-hatarozat.pdf, December 2019. (Accessed on 09/24/2021, translated to English by Google Translate).

[6] Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679, (Accessed on 09/24/2021).