Case Study on the Decision of the UK Information Commissioner to Fine Mermaids for Failure to Protect Data Subjects' Personal Data

Yang Xu
Brown University

Abstract

This case study reports on the decision of the Information Commissioner of the United Kingdom to fine Mermaids, a transgender rights charity £25,000 for failure to secure personal data under the provision of GDPR. It found that Mermaids, as the data controller, neglected to secure its internal email system, which caused personal information of 550 data subjects, many of whom children and vulnerable individuals, to be publicly accessible. In this report, I summarize the factual details of the case, especially after the breach was reported, and the legal basis for this decision as presented in the decision. I also discuss my personal assessment of the handling and the significance of the case.

1 Introduction

On July 5, 2021, the Information Commissioner ("the Commissioner"), the data protection agency of the United Kingdom (UK), issued a decision (the Decision) to impose an administrative fine on Mermaids, a charitable organization head-quartered in Leeds, UK that helps gender-diverse children and youths [3], in the amount of £25,000 [4]. The Commissioner found that Mermaids failed to implement sufficient organizational and technological security measures to protect its internal email systems between May 25, 2018 and June 14, 2019, which resulted in personal data of 550 data subjects being exposed, including that of children and in some cases special category data, which violated Articles 5(1)(f) and 32(1) and 32(2) of the GDPR. This case study reports the factual background, summarizes the details of the contravention, and discusses the appropriateness of the Decision.

2 Factual Background

Originally a support group for parents whose children are experiencing gender incongruence, Mermaids became a registered charity in 2015 to support kids, youths, and their families on issues related to gender non-conformity [4]. On June 14, 2019, a service member of Mermaids reported to its Chief Executive Officer (CEO) of internal emails being made available publicly. The CEO immediately informed the Commissioner of the breach on the same day. 3 days later, the CEO briefed the Commissioner on the phone about the steps Mermaids had taken in response to the breach.

Further investigation by the Commissioner revealed that the CEO of Mermaids created an email group with a third-party processor located in the United States called Groups.IO (`https://groups.io`) to share emails between the CEO and the 12 trustees. Since the group's creation on August 15, 2016, the security and privacy setting on the group had been left at the default "Group listed in directory, publicly viewable messages" value, which made the emails exchanged in this group between its date of creation and the last active date July 21, 2017 publicly accessible and searchable even after the group became inactive, until the CEO was notified of the breach. By this time, it was determined that breach involved personal data from 550 data subjects, of whom 24 data subjects had data that was sensitive/pertained to children or vulnerable individuals.

This violation could have been prevented if the default privacy setting of Group.IO were the most instead of the least secure option. However, the CEO him/herself could have exercised more caution before using email groups with full knowledge of the sensitive nature of the personal data and reviewed the privacy settings of the group.

3 Legal Basis for the Decision

This case falls under the jurisdiction of GDPR because the email group in question was still in operation after GDPR came into effect on May 25, 2018 until the report of the breach on June 14, 2019, when the UK was still a member state of the European Union (EU). Therefore, this case is purely internal to an EU country (at the time of violation). Article 83 of GDPR grants the data protection agencies the member states legal authority in seeking monetary penalties for violations of GDPR. In this case, the Information Commissioner is the

agency in UK exercising such power.

The data subjects of the case are the 550 individuals whose personal data was exposed. Article 4(1) of GDPR broadly defines any identified or identifiable information pertaining to a natural person who can be directly or indirectly identified. The personal data involved here includes but is not limited to names, email addresses, private emails and messages, and perhaps most importantly, gender identity and/or sexual orientation, which falls under "special categories of personal data" on which GDPR prohibits any processing unless certain requirements are met under Article 9.

Under the definition of GDPR Article 4(7). Mermaids is the data controller and processor, because it collects personal data, determines the purpose of the processing of the data [4], and processes the data itself. Groups.IO is also a data processor because it processes personal data at the request of Mermaids. However, Mermaids was the only organization held accountable in the role of the data controller according to Article 5(2).

Mermaids violated GDPR Article 5(1)(f) because it failed to process the data "in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing ..., using appropriate technical or organizational measures ('integrity and confidentiality')." [2]. Although not specified by the Decision, it could have also violated Article 5(1)(e) because it kept identifiable personal data in a format longer than necessary and left the email group dormant after it stopped using the group.

Mermaids' contravention also infringed Article 32(1)(a), (b) and (d) because it failed as the data controller to use pseudonymisation and encryption on personal data, ensure the confidentiality of the data, and adopt regular evaluation of its technical and organizational measures it takes to ensure security of processing. In addition, Article 32(2) was violated because Mermaids neglected to assess the appropriate level of security with regard to the the level of risk involved in the event of unauthorized disclosure given the sensitive nature of the personal data that they processed [2].

4 Remedial Actions

In addition to immediately informing the Commissioner of the breach, Mermaids was also cooperative and took remedial actions following the discovery of the breach [4], including:

- On June 14, 2019, the day they were made aware of the breach, it changed the security setting of the email group in question to private and started reviewing the emails which had been exposed.
- On June 15, 2019, it started informing data subjects whose data they deem "sensitive," of the breach and disclosed to them what personal data was exposed, beginning with those whose contact information it could locate. it also acknowledged and apologized for the incident on their website.
- On June 17, 2019, it hired a data protection consultant and started the process of removing the exposed data online, including sending request to Google and Archive.li for removal of cached and archived information, and contacting Group.IO to delete any sensitive information in their logs.

Considering the swift actions taken, it seems that Mermaids did take appropriate actions to timely inform the authority and the data subjects of the details of the breach and adopt appropriate remedial measures to remove exposed data online.

5 Regulator Actions

Because Mermaids was proactive in reporting the breach and taking remedial actions immediately following the breach, the Commissioner mostly remained in the background and worked with Mermaids to ensure that all appropriate measures were taken. After the immediate aftermath, however, the Commissioner conducted thorough investigations of the incident of the breach and notified Mermaids of its intent to impose a monetary fine on March 9, 2021, approximately 9 months after it was made aware of the incident. The final Decision was issued on the Commissioner's website on July 5, 2021, less than a year after the incident [4]. The language used in the Decision is non-technical both in the legal and technological sense, easy for non-technical audiences, probably also because the legal and technological issues involved in this incident are not excessively technical. In the Decision, the Commissioner clearly delineates the timeline of the incident and specifies the articles in GDPR that were violated. She also clearly outlines how a fine of the amount £25,000 was reached, considering the gravity of the violation, the potential harm to the data subjects, the remedial actions Mermaids took, and the nature of Mermaids as a charitable organization.

The Commissioner has announced no further actions taken against Mermaids since, indicating that Mermaids has most likely paid the monetary fine.

6 Discussion

Even though it is no small amount for a charitable organization [1], £25,000 is appropriate especially considering the sensitive nature of the personal data involved and the potential harm that the breach could cause. As is mentioned in the Decision [4], gender incongruence is still a controversial and extremely sensitive topic, and Mermaids' negligence in securing such sensitive information could potentially lead to trauma for the individuals that it is supposed to protect.

Such a fine could be a cautionary tale for other charitable organizations, especially those dealing with sensitive issues,

because the negligence of Mermaids could be commonplace among similar organizations. They typically rely on donations to operate and may not hire data privacy consultants to secure their data due to limited operational funds. They might also focus more on charitable practices than on technical issues such as data security, which gives more reason to highlight the issue of privacy and security.

Although this process documented in the Decision generally worked well, Group.IO notably was not held liable at all. Although it is not justified to impose a fine on them, actions should be taken to ensure that developers "err on the side of caution" and provide maximum security options by default. Had they followed this principle, this entire incident might have been prevented.

One such solutions might be a provision in privacy laws that requires maximum security options by default to prevent such incidents from happening. Violators of such principles might share a small portion of the liability, even though the data controller should still bear the majority of the blame.

References

[1] DAC Beachcroft. £25,000 ico fine is no drop in the ocean for mermaids, June 2021.

[2] The European Commission. General data protection regulation (gdpr), Sep 2019.

[3] Mermaids. Mermaids website, Sep 2021.

[4] The Information Commissioner's Office. Data protection act 2018 (part 6, section 155) supervisory power of the information commissioner monetary penalty notice. Jul 2021.