# Is Your Work Email Yours? A GDPR Case Study

Mary McGrath
*Brown University*

## 1 Introduction

An Italian chemical products company [2], Mapei SpA, was fined €15,000 by Garante per la Protezione dei Dati Personali (Garante) for the violation of Mr. XX's rights under the GDPR. Mr. XX left Mapei's employment on July 31, 2017, however, Mapei kept the individual email of Mr. XX active with all incoming messages forwarded to his immediate supervisor at the time his employment ended. Mr. XX was unaware that his prior email was still active until he performed a test seven months later which showed the account was still active. Garante found that Mapei violated the principles relating to processing of personal data as well as those relating to disclosure of and access to the data. [6]

## 2 Background

Mr. XX, the data subject, was employed at Mapei SpA, the data controller, until July 31, 2017. Upon termination of the employment relationship, Mapei took steps to recover IT equipment and disable user accounts. However, the individual email account for Mr. XX was left enabled with a rule to forward all emails to his direct supervisor at the time of his employment.

Mapei left the email of Mr.XX enabled post-employment to ensure the continuity of business operations. The company argued that the email, per their policy, is solely for the use of professional correspondence and therefore 1) it is not personal data, and 2) it is the under the company's purview to keep using it for business purposes.

This raises the question of whether a work email is personal data. Garante, Italy's data protection authority, had previously found that using an individual email after a consulting relationship had ended was not allowed under a pre-GDPR Italian privacy law [1, 5]. One of the points argued in that case [1], which was not raised in this case [6], was that the name in the email address was inherently personal data. However, both argued that the contents of email, while professional, also represent personal relationships and communication. Additionally, it was argued that the senders of the email have rights and a reasonable belief that the correspondence is confidential, which is not upheld in the case of this forwarding to a third party.

## 3 GDPR Violation

The following articles of the GDPR [4] were found to have been violated:

**Article 5** Principles relating to processing of personal data

- (1)(a) lawfulness, fairness and transparency
- (1)(c) data minimisation
- (1)(e) storage limitation

**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 of access by the data subject

### 3.1 What Happened?

Mr. XX left the employment of Mapei on July 31, 2017. In February 2018, he found that his individual email account at Mapei was still active and being forwarded to his prior supervisor. In April of 2018, he filed a GDPR request to access the emails received since July, 2017 and for the email inbox to be disabled. No response was received, so a reiteration of the request was sent in July of 2018. Lawyers for Mr. XX raised a complaint to Garante in August 2018. In October of 2018, Garante sent a request for information to Mapei, to which Mapei replied in November stating they believed they were in the right as the email was for business purposes and no personal data was involved. At that point, they sent Mr. XX's lawyers a copy of the emails sent to the email from the time of termination to the time of the inbox's deletion. Mr. XX rebutted the claims of Mapei, noting there was a large gap of missing emails from March through June of 2018 and asserting that the policy Mapei was citing in regards to their usage of the individual email post-termination was never provided to Mr. XX. In September 2019, Garante notified Mapei of the alleged violations and held a hearing on December 3, 2019. The injunction against Mapei was issued July 2nd, 2020.

Mapei was found to have violated several articles of the GDPR. According to the injunction, the most egregious of the violations were those related to the principles of data processing (Article 5). They found that Mapei did not act transparently in keeping this inbox open without explicit notification to Mr. XX, did not minimize the personal data of Mr. XX, and in keeping the inbox open for 10 months post-employment exceeded reasonable limits for storing data for the minimum period necessary. In addition to the Article 5 violations, Garante also found that Mr. XX's rights to access his data was violated due to the company's non-response to his GDPR request, thus violating Articles 12 and 15. The company also did not fulfill their duties as a data controller to communicate with the data subject, Mr. XX, the use of his data per Article 13.

## 3.2 Who/What is Responsible?

This violation is largely a failure of human judgement and policy, though technology may be useful in enforcing a better policy. The company purposefully left the inbox of Mr. XX enabled and set up a forwarding rule to the supervisor. This was per their policy at the time. It was Mapei's view that forwarding the emails was the best solution to allow for continuity of business relationships after Mr. XX left the company.

The violation of Article 12, which resulted from Mapei's non-response to the GDPR request of Mr. XX could have potentially been avoided with technology. Mapei now has a GDPR request form [3], but I am unable to find if it was in existence in 2018. The company could implement tools to better track these requests and make sure they are all responded to (which includes negative responses) in a timely manner.

## 3.3 What could have prevented this?

A different solution that would maintain business continuity and protect the personal data of subjects would be to have the email address auto-reply to the sender without storing the contents of the email. This could both let them know that Mr. XX was no longer working at Mapei and whom they should contact in his stead. This is now Mapei's policy as of September 2019. This solution was also recommended by Garante in the provision against Jenny.Avvocati [5].

# 4 Discussion

While this has not been a high profile case (no press releases or news articles could be found), it represents a reaffirmation that data created in the course of business can also be personal data and must be treated as such. Work email is a murky territory wherein it is for business purposes, and all IT policies will say as much, however the personality and personal information of the correspondents is imbued in it over time. This case has found that work email is personal data that a data subject has rights to under GDPR and that a data controller (employer) must treat it as such in responding to GDPR requests. This case also establishes that even storing and forwarding an email within an organization without the consent of the data subject constitutes processing beyond the scope of the principles of processing personal data (Article 5).

The fine of €15,000 appears to be relatively high given that the data subject is a single person. However, I believe this is appropriate given the broad nature of the violation and that email has a general expectation of confidentiality even within an employee-employer relationship. It is also important to establish that this type of policy is not appropriate and to deter other companies from doing this. It is likely somewhat common, especially in smaller companies, as setting up email forwarding is technically quite simple, whereas other solutions require more technical implementations.

In conclusion, your work email is mostly yours.

# References

[1] Italian personal data protection code. https://www.unodc.org/res/cld/document/ita/2003/personal-data-protection-code_html/Italian_Personal_Data_Protection_Code_-_Legislative_Decree_no_196_2003.pdf. Accessed: 2020-09-24.

[2] Mapei. https://www.mapei.com/it/en/home-page. Accessed: 2020-09-24.

[3] Mapei gdpr request form. https://privacyportal-eu-cdn.onetrust.com/dsarwebform/a4bfd8d0-8fa6-4d7d-8417-fd634984d69e/669e7015-5fb5-473f-a1ee-18265339e0db.html. Accessed: 2020-09-24.

[4] Council of European Union. Regulation (eu) 2016/679 of the european parliament and of the council, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.

[5] Garante per la Protezione dei Dati Personali. Provision of 5 march 2015, 2015. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3985524.

[6] Garante per la Protezione dei Dati Personali. Injunction order against mapei spa - 2 july 2020, 2020. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445180.