GDPR Case Study
- A Merseburger's Mailing List

Introduction

This case study looks at a violation done by a private person, instead of a global tech company. The violator exposed personal email addresses of every recipient on his mailing list to other recipients. Offenses to the GDPR as such happened more than one time. The aim of this case study is to give an overview of what happened, examine how GDPR was violated , and discuss the impact of this case. Additionally, the means of detecting such violation used by law enforcers will be discussed.

Background

Regulators of the State Commissioner for Data Protection in Saxony-Anhalt have charged a resident in Merseburg of a violation of the GDPR between July 2018 to September 2018. The Merseburger maintained a mailing list, as large as 1,600 at times, which he used to send "complaints, statements, denunciations but also criminal charges against the most diverse representatives of the economy, press, local and state politics."[1] The content of his emails was not the cause for a fine of 2,685 Euros, issued on February 5th, 2019. The person violated the GDPR by exposing personal data, without consent.

GDPR Violation

When sending daily emails, the violator used all email addresses on his mailing list in the recipient section, causing all recipients to see other recipients' personal email addresses. The recipients other than the person viewing the email will be addressed as co-recipients in the following paragraphs.

The data subjects of this case are the individuals on the violator's mailing list. The data controller is the violator. The data processor is the email service provider. Since this case only concerns a private person, the infrastructure used was only the personal computer of the violator and infrastructures used by the email service provider.

Since media reports disclosed little information on how regulators detected such violation, an assumption is necessary to continue discussion. The content of the email, described in section 2, was somewhat of interest to the authorities in Germany, so this violator could have been on the authority's notice before this violation occurred. Once the violation was detected, regulators conducted an investigation and issued a fine of 2,685 euros in February, 2019.

In this case, Article 6 of the GDPR had been violated. Since the mailing list was maintained only for the purpose of giving information, none of the items (b) - (f) were satisfied. Due to the fact that the violator did not acquire consent from data subjects to make their email addresses visible to other

[1] https://www.mz-web.de/merseburg/hunderte-adressen-im-verteiler-merseburger-muss-fuer-wut-mails-ueber-2-000-euro-zahlen-32033308

subjects on the mailing list, item (a) of Article 6 was violated.

From a purely legal perspective, the mailing list owner was responsible for the privacy and security of personal email addresses of the data subjects. However, not masking co-recipients' email addresses is a common practice. Since GDPR only became effective in May 2018, both the violator and his email service provider had little time to react. In this case, the violator's "slow" sense of keeping up with the GDPR was the only human factor. However, the data processor should have shouldered more responsibility.

Take the example of Gmail, one of the most popular email service providers. When a person sends an email to multiple recipients, Gmail will show a drop down button which, upon clicking, will show you the email addresses of co-recipients. This is not an intentional choice for "privacy intrusion", but rather a UI design choice made by Google. With this understanding in mind, the violator in the case of this article seems to have no control over whether a recipient could view other co-recipients' personal email address.

To avoid this violation in the future, the sender could send each recipient the same email, instead of writing one email, adding all recipients on a mailing list, and clicking send. However, if the mailing list is sufficiently large, it is not feasible for the avoidance of such violation to fall on the user. Email service provider should instead show email addresses of the sender and the CC'd recipients.

Discussion

Although this case only concerns one individual, it raises some interesting questions.

First, who is really responsible for this violation? As discussed in the last two paragraphs of the GDPR violation section, the violator himself may or may not have direct control over whether recipients can see each other's email addresses. Since this is beyond the control of any individual user, email service providers should take actions to modify the design of email service front end privacy setting to mask the email addresses of co-recipients.

Secondly, how did the regulators find out about this offense? The nature of the violators' email provides some implications for this case. If a recipient on his mailing list reported this offense, it will be a simpler case. However, if the regulator detected this violation, a scary assumption can be made -- the government might be tapping into the email service provider's data center to view emails.

With these two questions in mind, readers should reconsider how GDPR compliance should be maintained. Maybe it is time to elaborate more on the execution and investigation of GDPR and put authorities in check.

[1] https://www.mz-web.de/merseburg/hunderte-adressen-im-verteiler-merseburger-muss-fuer-wut-mails-ueber-2-000-euro-zahlen-32033308