GDPR Violation Case Study: Roma Capitale

Koyena Pal
Brown University

Abstract

On July 22, 2021, the Italian DPA, ruled that Roma Capitale (Rome) was improperly managing personal data collected at parking stops in the city. Their actions were ruled as violations of GDPR articles 5,12,13,25, and 32. As a result of their non-compliance, Rome was fined €800,000. In addition, the service company, Atac s.p.a. and sub-provider Flowbird Italia s.r.l. were also fined €400,000 and €30,000 respectively for not protecting personal data of drivers that parked in the Rome Municipality territory.

1 Background

After receiving an individual's complaint on the new parking meters installed in Rome in 2018, the Garante, Italian DPA, began investigating the Municipality and their contractors (companies that provided and maintained the parking meters) on how they use and handle the driver's personal data. By doing so, the DPA realized that the city of Rome, "had not provided information on the processing of the drivers' data" [4]. In addition, they realized that the companies that maintained the parking meters were not established as data processors and there was no "data processing register" [4] or instructions set on how to process the personal data collected from these meters. This issue results in the following parties being involved:

Data Controller: Roma Capitale or city of Rome is responsible for managing personal data of the drivers parking in the city. They should instruct what and how the data should be collected and processed to the data processors. In addition, they should also be able to communicate and allow users and regulators to provide related information on what data is collected and how it is being used and secured.

Data Processor: Atac S.p.a.'s equipment were used to operate the parking meters. They also sub-contracted with Flowbird Italia S.r.l for parts of the equipment. Atac was tasked with processing parking meter related information and making sure that users were paying for the space they parked at. However, they had an insecure way of storing these data and continued to store them with no clear sign on when they would delete it. Both Atac and Flowbird should have upheld the responsibilities of being data processors of Roma Capitale. Based on the decision report ([3]), "Roma Capitale stated that "having no relationship with said parties [...] it has not formulated any appointment as responsible for said parties." This means that the data controller and processor relationship was not really established.

Data Subject: All users who paid for the parking service in the city of Rome area are affected. "From June 2018 to November 2019, the system established by Atac had already collected the data of 8,600,000 stops" [1]. Hence, at least all users from all of these stops are affected by this violation. The data being mishandled included time, date of start and end of parking, the amount paid and the license plate.

2 GDPR Violations

Ultimately, it was ruled that Roma Capitale was in violations involving processing of personal data, transparency information and communication of personal data to data subjects, as well as data protection by design and default. Specifically, this involves articles 5,12,13,25, and 32.

2.1 The Infringements

The overall infringements on GDPR regulations committed by Rome falls into 3 main categories:

Lack of communication with data processors and vice-versa: Without establishing the data controller-data processor relationship and specifying what is expected out of the data and how to process it, situations like these arise where the expectations of the data controller and data processor becomes unclear to the parties. Based on the decision report, the companies had not planned the data processing registry. Looking at the database, the Garante realized that Atac retained all the data collected from parking meters and were also stored in an unsecure manner. This realizes the next infringement.

Poor security and storage of data In the decision report, the following was detailed: “In the dbo.Multe table, in which the information relating to fines raised by traffic auxiliaries is stored, the information relating to the license plate is stored in clear text for about 60 days. In the dbo.sostaInizio table, the data relating to the period of validity of a payment (date, time of start and end of parking, vehicle plate, etc.) are stored. Out of the aforementioned data, only those relating to the last 60 days are stored in clear text." [3] In addition, using the “Movements" detail function, it was plausible to find routes and locations of users with their license plates. This hinders the physical security of the users.

Lack of transparency to data subjects As data subjects, the drivers have the right to request how their data is being used and processed. Due to the lack of communication and lack of logs to retrace the user, it is difficult for the data controller to pass this information.

2.2 Ruling and Response

Roma Capitale was found to be in violation of GDPR and was fined €800,000. In addition, the service company, Atac s.p.a. and sub-provider Flowbird Italia s.r.l. were also fined €400,000 and €30,000 respectively. Since the ruling was held pretty recently, the response is still unclear. Nevertheless, the decision does include some preventive measures (such as content hashing, secure gateway (https instead of http) to help both data controllers and data processors to improve their communication and technical abilities.

3 Discussion

Given the amount of data compromised, the fine imposed seems to be low. If we were to include all the data controller and processor charges, it would be a little over a million euros. In context to how many stops' data were stored indefinitely (at least 8,600,000), each stop's data (which includes many drivers' data) is worth less than a euro compared to the charges. Furthermore, even if this incident has occurred only in the EU, it is possible that non-EU citizens may be affected. Examples include tourists who drove by and parked at the stops at Rome. In addition, there was a similar violation conducted by the Municipality of Rome through another system called “TuPassi" [2]. Hence, a couple ways to reduce such violations is to publicise these reports more (not just locally, but globally). In addition, as researchers, we should create more GDPR-friendly software and privacy-conscious computer systems that can be autonomous, easy-to-install and re-purposed for services such as parking meters.

References

[1] CA/IN. Interesting case of roma capitale, 2021. [Online; accessed 25-September-2021].

[2] GDPRhub. Garante per la protezione dei dati personali - 9524175 — gdprhub,, 2021. [Online; accessed 25-September-2021].

[3] Register of measures. Injunction order against roma capitale - july 22, 2021 [9698724], 2021. [Online; accessed 25-September-2021].

[4] Enforcement Tracker. Gdpr enforcement tracker, 2021. [Online; accessed 25-September-2021].