When Telemarketing Goes Too Far: A GDPR Case Study on TIM

Casey Nelson, *Brown University*

Abstract

On January 15, 2020, the DPA supervisory authority, Garante, ruled that TIM, an Italian telecommunications company, was improperly managing consent to use subject's data in promotional activities. Their actions were ruled as violations of GDPR articles 5, 6, 7, 17, and 21. Additionally, it was ruled that TIM was not properly responding to data breaches, which is in violation of article 33. As a result of their infringements, TIM was fined €27,802,496. In addition to their fines, TIM was also given 20 corrective measures which they had to instate in order to meet GDPR compliance.

1. Background

After receiving an abundance of complaints for excessive promotional calls from TIM between 2017 and 2019, the Italian SA, Garante, began investigating TIM and their "partner" companies (companies to which TIM outsources their telemarketing calls) for a misuse of both customer and non-customer data [1]. The complaints reported receiving TIM promotional calls up to 155 times a month despite already declining a specific promotional offer, opting out of promotions all together, or not even being a direct TIMs customer [2]. This reveals a failure on TIM's behalf in terms of properly managing opt-ins for promotional activities, which violates the right of data subjects to consent or dissent to any particular usage of their data.

The parties involved in this problem setting were the following:

Data Controller: TIM, the Italian telecommunications company, was responsible for managing their customer's data and dictating how it should be used for promotional activities.

Data Processor(s): TIM's unidentified "partners", were tasked with processing data for promotions. The "partners" were telemarketing companies responsible for using the data TIM provides, mixed with some in house data they've collected, to make promotional calls on TIM's behalf [1]. Additionally, TIM should have been responsible for managing the data it distributes across its partners to make sure updates, such as opt-outs, were recorded and reflected in all of their partner's databases.

Data Subjects: The data subjects were a mix of millions of TIM's customers as well as non-customers whose data was being misused for promotional purposes. The data being abused included name, address, phone number, tax code, and other contact details [1].

2. GDPR Violations

Ultimately, it was ruled that TIM was in violation of GDPR articles involving an individual's ability to give and opt out of consent as well as timely handling of data breaches. Specifically, this involves articles 5, 6, 7, 17, 21, and 33 [5].

2.1: The Infringements

The overall infringements on GDPR regulations committed by TIM falls into 4 main categories:

1. *Poor management of blacklists across TIM and its partners*: TIM uses blacklists, lists of customers who wish to not have their data used for marketing activities, to regulate their promotional calls. TIM uses 2 separate lists to manage this. The first is the marketing blacklist, which contains the list of individuals who expressed to customer service that they would like to be excluded from all promotional activities. The second is the denial blacklist, which contains a list of individuals who denied participation in promotions during a telemarketing call [1]. However, during the investigation, it was found that there were many discrepancies across TIM's blacklists and the blacklists used by TIM's partners. TIM blamed these discrepancies on the fact that all over the phone denials must be manually logged by the partner into a central database to be added to the global denial blacklist [1]. Supposedly, partner companies were updating their own internal blacklists but not the denial blacklist. Thus, despite opting out of promotions with one partner, an individual's data could still be processed and used for promotional means by another partner. The failure on TIM's behalf to properly control the activities of their partner companies was viewed as a GDPR violation. Specifically, this infringement violates article 17.1.b as the data controller is responsible for properly removing a subject's data if they terminate their consent [5].
2. *Violating the duration of storage and usage for secondary customers' data:* Under TIM's contract, they have the right to store the data of secondary

customers, individuals who purchased TIM products from other licensed operators, for up to 10 years. For the first 5 years they are permitted to use the data for customer service reasons; however, they are allowed to store it up to 10 years for tax purposes only [1]. During the investigation, it was found that TIM was storing secondary customer's data beyond this 10 year period and were using it for marketing purposes, which is outside of the scope to which secondary customers consent [1]. This is in violation of GDPR articles 5.1.b,e as well as 17.1.a since the data was both used and stored outside of its specified scope [5].

3. *Improper means of obtaining consent for promotional usage of data:* TIM's means of obtaining consent to use customer's data for marketing purposes violated GDPR article 7 on two counts. The first violation was the fact that they required that customers consented to having their data used for promotional means in order to join "TIM Party", a discount service [1]. This was seen as violating article 7.4 since the use of customer's data for promotional purposes did not relate to the ability for "TIM Party" to carry out its service [5]. The second violation was due to the fact that TIM hid consent to use customer data for promotional purposes in the terms and conditions for many of their apps. This is in violation of article 7.2 since requests for consent within documents concerning multiple matters must be made clear and distinguishable [1][5].
4. *Failure to timely notify supervisor of data breaches:* Unrelated to the notion of consent, TIM was also found to be in violation of GDPR article 33 for not following the proper timeline in terms of notifying their supervisor of data breaches [2].

2.2: The Ruling

TIM was found to be in violation of GDPR and was fined €27,802,496 [1]. Additionally, TIM was given 20 corrective actions which they had to fulfill to meet GDPR specifications. Broadly, this includes no longer using the data of subjects who either denied promotional calls, asked to be added to blacklists, or any non-customer who did not consent the use of their data for marketing. Additionally, they can no longer use any of the data they previously collected through their apps [2].

2.3: The Response

TIM did very little to address their GDPR infringements publicly. There was a press release in April, 4 months after the conclusion of their case asserting that "respecting privacy regulations is a priority" and describing all the ways in which they comply with GDPR [3]. However, as an interesting note, all of the GDPR compliance changes that TIM lists in this press release were initiated prior to their GDPR case ruling.

However, that is not to say that TIM's GDPR violations went unpublicized. Details of their infringements, in layman terms, can be found in a plethora of articles as it is one of the top 5 GDPR fines in 2020 [4]. In general, these articles make the big picture of TIM's GDPR violations known to the general public. However, they typically omit specific article violations and technical details.

2.4: Prevention

TIM's biggest issue was that they failed to have a robust management system over their data across multiple partners (the data processors). Namely, TIM did not have an efficient system for propagating a subject's decision to opt out of promotions across their multiple partners. When a subject opted out of promotional calls with a specific partner, that partner would have to manually upload this change to the global database, which they often failed to do [1]. To help better facilitate this process, TIM could have developed a system such that there exists only one copy of each customer's data so that multiple copies do not have to be maintained across multiple partners. Alternatively, a system of partitioning their customers so that the same subject's data was not given to multiple partner companies would also achieve this goal. With a partitioned database, changes to one subject's status would not be relevant to other partner's. Additionally, this technique has the benefit of sharing a subject's data with a minimal amount of outside sources.

Another issue was the general lack of knowledge on TIM's part as to what their partner's were doing with the data they were processing. There seemed to be a lack of clear communication between TIM and its partner's which presumably caused the partner's to act outside of their instruction. However, it seems questionable whether this lack of clear communication was a mistake or a deliberate attempt to over step their bounds on subjects' data without being blatant.

3: Discussion

Given the scope and manner of TIM's GDPR infractions, the fine imposed seems reasonable. Millions of individuals, both customers and non-customers, were victims of unlawful data processing for TIM's promotional needs. Additionally, the manner of TIM's infractions come across as being either neglect or a deliberate attempt to hide unwarranted data processing.

The magnitude of the fine imposed in TIM is even more justified by considering the fact that this is not TIM's first

GDPR violation. They were previously fined, again by Garante, back in 2018 immediately after the approval of GDPR [6]. In TIM's prior GDPR infringement, they were, among other violations, charged with unlawful processing of erroneous client data, which is in violation of article 5.1.d [5][6]. This is particularly relevant to their more recent GDPR violation as it follows the same theme of unlawful processing due to neglect from a data management perspective.

Overall, TIM's second GDPR violation is important because it demonstrates to companies that they must always be vigilant in maintaining GDPR violations. Responding to one offense does not make a company clear for life.

References:

[1] Garante. *Provvedimento correttivo e sanzionatorio nei confronti di TIM S.p.A*. 15 January 2020.

[2] European Data Protection Board. *The Italian SA Fines TIM Eur 27.8 Million*. 1 February 2020.

[3] Gruppo TIM. *Privacy and e-Security: Safeguarding Privacy and Personal Data Protection*. 5 April 2020.

[4] Data Privacy Manager. *5 Biggest GDPR Fines of 2020 [So Far]*. 18 August 2020.

[5] European Parliament and the European Union. *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. 4 May 2016.

[6] Pappalardo, Massimiliano. *Lessons to be learnt from Garante's fines against TIM*. Studio Legale D&P. June 2018