Analysis of UOOU GDPR Charges Against "Car Rental Company"

Sam Thomas
CSCI 2390

Abstract

In February 2019, the UOOU (Czech Data Protection Agency) filed charges against an unnamed car rental company for violating the GDPR. The UOOU cites that personal data was not "processed correctly and in a lawful and transparent manner," which was a violation of Article 5, Section 1 of the GDPR. In particular, the car rental company tracked GPS data that was associated with data that qualifies as identifiable and traceable to the data subjects involved. The UOOU fined the car rental company €1165, which equates to 30,000 Czech crowns, and was forced to transfer the fine to a specified bank account within 30 days.

1 Introduction

In one of Europe's first GDPR charges, the UOOU (which is the Czech Data Protection Agency) fined a car rental company €1165, or 30,000 Czech crowns, for violating Article 5, Section 1 of the GDPR. The case was brought to the UOOU after a complaint from a car rental customer who recognized that, despite not being notified, their GPS data was being stored. Upon investigation, the UOOU determined that the GPS data, along with several other fields, was being stored in an identifiable. The UOOU deemed this practice to be a violation of the principle that personal data should be "processed correctly and in a lawful and transparent manner." [6].

In Section 2, this paper will discuss: the data protection agency (DPA) responsible for charging the responsible party, the data subjects, data controller, and data processor, and data architecture. In Section 3, this paper will discuss the particulars of what happened, the parties that were responsible for the violation, and any measures that could have been taken to avoid the violation. In Section 4, this paper will discuss my personal opinions on the case.

2 Background

Data Protection Agency

A Czech car rental company was fined by the UOOU, which is the *Czech Data Protection Agency*, who was the responsible DPA heading the case. The case involved European Union citizens with in the physical jurisdiction of the European Union.

Involved Parties

According to [6], several columns of data from "natural persons" was stored in what can be assumed to be a central data storage. This data "undoubtedly" includes "name, surname, address, telephone number, tenant's ID card number and also name, surname driver and his driver's license number, IP address, e-mail address and GPS position of the motor vehicles, as this information can clearly be related to a specific data subjects." From this point, these classes will be considered *data columns*. The *data subjects* referred to in the quote are the natural persons whose data is being stored. These are primarily, if not entirely, customers of the car rental company who rent cars.

In this case, the *data controller* and *data processor* are the same party - namely, the car rental company. This is because the car rental company dictates the

terms of the data usage and also defines itself as in charge of the storage and usage of the data itself.

Architecture

As such, it can be assumed that the architecture used was a central online service through which natural persons can register to rent a car. Before personal data is submitted to the central data storage, the customers should be promted to agree to the conditions that data is stored in the central data service. However, as will be discussed in 3, the terms of the GPS data was not conveyed in these conditions.

3 GDPR Violation

What Happened

As stated in Article 5, Section 1 of the GDPR, personal data must be "processed correctly and in a lawful and transparent manner." However, the car rental company was processing GPS data to track the location of customers and the car during the rental period. This data was identifiable to data subjects through several columns of data (including name, surname, e-mail address, etc…). Furthermore, the use of this data was not part of the rental terms, meaning that customers did not consent to having the data processed in this way.

The violation was reported by a customer who, after renting from the car rental company, noted that the GPS data was being tracked and stored without having consented to this behavior. It is unclear how the customer became aware of such behavior, as the customer's identity remains anonymous in [6].

After the complaint was filed to the UOOU (Czech Data Protection Agency), a thorough investigation took place which demonstrated that such actions were in fact a violation of the GDPR. Furthermore, they determined that the behavior took place from at least May 24, 2018 to October 23, 2018 (about five months). The UOOU received the initial complain on June 21, 2018 and imposed fines on February 4, 2019, which means that the investigation took over seven months to complete.

Responsible Parties and Preventability

The act of collecting GPS location data while customers rented cars in and of itself was not a GDPR violation. Instead, what made the action unlawful was that (1) the location data was identifiable to particular data subjects and (2) the processing of such data was not consented to by data subjects in advance of the data collection.

The first point is a technical flaw. If the data was tracked and stored such that it was not identifiable to particular data subjects (i.e., the data was stored separate from customer data columns with encrypted/random identifiers or no identifiers at all), then this condition would prevent the GDPR violation.

The second point is a human flaw. If the processing of GPS data was explicitly described in advance of car rentals and agreed upon by the data subjects, then no such violation would take place. That is, the violation could have been reprimanded by having more explicit terms of use. Either or both solutions would ensure that the circumstances do not violate the GDPR, however as it stood the case was deemed to be "unlawful" processing of data.

4 Discussion

This was one of the first fines levied under the pretenses of the GDPR. As such, this case is important in that it helped set several precedents. In my opinion, these precedents can be summarized in three different perspectives: (1) establishing a definition for "unlawful" data processing, (2) providing anonymitiy for the car renting company and data subjects involved, and (3) leniancy in the levied fine amounts.

Through the mere legalese of the GDPR, the term "lawful data processing" is largely ambiguous without examples of what unlawful data processing would look like. This case is important in that it demonstrates one such example of unlawful data processing - namely processing identifiable data without the consent of the data subjects. What is interesting about this case is that both the terms "identifiable" and "consent" explicitly appear in the GDPR [1]. This

implies that lawful data processing is an umbrella term for upholding other standards explicitly mentioned elsewhere in the GDPR.

Again, due to the timeline of this case, it was important in establishing anonymity in the proceedings of official DPA reports after levying fines. Without more information, it's unclear as to the stature of the car rental company (car rental company local to Czech Republic vs. large international corporation). With this anonymity, the car rental company in question is able to preserve a positive public reputation. Though outside the scope of this paper, it would be interesting future work to study the anonymity of data subjects, data controllers, and data processors in other cases going forwards in the Czech Republic and elsewhere in the European Union.

Finally, according to [6] "the fine was imposed at the very lower limit of the rate provided for in Regulation (EU) 2016/679." This action establishes a precedent for the most lenient legal fine for companies like the anonymous car rental company who violate the GDPR. Out of purely speculation, the lower-end fine might be the result of the company being a smaller company, and any larger fine would hurt the company's future prospects. Alternatively, there may have been some form of side deal that may have been made with the UOOU to ensure that the penalty was not too severe. Either of these reasons may be why the car rental company has remained anonymous.

The UOOU report was full of legalese and redacted names and quotes. This could have been done for anonymity purposes, but made the document difficult to read. The case has been cited in news articles [4, 5] and GDPR cases datasets [2, 3] where short paraphrases of the case are provided, but details of the parties involved are limited as a result of the anonymity of the report. As such, it is difficult to make an anaylsis of the fallout of the case.

All in all, I believe that a case can be made that the handling of this case was either appropriate or inappropriate. Seeing as this case is one of the first examples of a fine being levied on behalf of the GDPR, one could argue that a conservative approach in the handling of this case - in defining ambiguous terms and the value of the fine itself - was appropriate given the circumstances. On the other hand, it is unclear as to why the minimum fine was levied and as to why the involved parties remained anonymous throughout the report. From the perspective that, without further information, this case seems to be a clear violation of the lawful processing of data spelled out in the GDPR and a full fine should have been imposed, this case would have been handled inappropriately. Personally, I tend to find the argument for the more conservative approach to be a compelling one in this instance.

References

[1] *2018 reform of EU data protection rules*. European Commission. May 25, 2018. URL: %5Curl%7Bhttps://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf%7D.

[2] *GDPR Enforcement Tracker*. Enforcement Tracker. URL: %5Curl%7Bhttps://www.enforcementtracker.com%7D.

[3] *GDPR Fines*. GDPR Fines. URL: %5Curl%7Bhttps://gdpr-fines.inplp.com/list/%7D.

[4] *Penalty against car rental*. EasyGDPR. URL: %5Curl%7Bhttps://easygdpr.eu/gdpr-incident/penalty-against-car-rental/%7D.

[5] *Personal Data Protection Office imposes first fines for GDPR breaches*. Danvoky. URL: %5Curl%7Bhttps://danovky.cz/en/personal-data-protection-office-imposes-first-fines-for-gdpr-breaches%7D.

[6] Ing. Josef Vacula. *Návrh*. 2019. URL: %5Curl%7Bhttps://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34465%7D.