

GDPR Violation Case Study: Google LLC

Atlas Yu
Brown University

Abstract

Data privacy has been a significant problem in the 21st century. Users, bombarded by ‘personalized’ ads, are often not aware of how their online activities are recorded into user profiles and sold to ad platforms as products. The ad business has been so lucrative that some companies even go out of their way to unethically obtain user data and eventually be punished for violating the General Data Protection Regulation (GDPR). There is no lack of successful large tech companies among the list, which has made negative impact on a very large scale. One of those large companies is GOOGLE LLC, which was fined 50 million euros for multiple violations of GDPR on 21st January, 2019 by the French Data Regulator, the National Data Protection Commission (CNIL). [3]

1. Background

Google, known as the largest search engine, is also the largest online ads platform in the world. Google generates advertising revenue through its Google Ads platform, which contributed about 134.81 billion US dollars in 2019, almost 70.9% of the company’s total revenue. [2] In order to make advertising effective and lucrative, ads platforms, including Google, have to figure out what are the best relevant ads to show each user. For instance, a college student might be interested in college related products, such as desk lamps, but less likely to purchase luxury cars due to financial situation. Therefore ads that are relevant to college life are more likely to lead to a sell, if the ads platform can figure out that the user is indeed in college. And the better the platform can understand users, the more likely they will make successful ads recommendations and the more money they will make. To better understand the users, ads platforms often need to collect personal data from the users, including their age, gender, location etc., so that the system would know how the person is feeling, what he or she is doing, and what the user might need to buy.

However, not all the people are comfortable with disclosing personal data and receiving tailored ads. To protect user’s privacy and personal data, lawmakers from the European Union established the General Data Protection Regulation (GDPR) to shield users from unwanted collection and use of personal data. Since the GDPR was implemented, there has been a growing list of individuals and companies that violated the regulation and faced serious financial punishments, the most severe of which was Google LLC, which was sanctioned for 50 million euros, the upper sanction limit from GDPR. [1]

2. Violation Detail

On 25 and 28 May 2018, the National Data Protection Commission (CNIL) received group complaints from the associations *None Of Your Business* (NOYB) and *La Quadrature du Net* (LQDN), French advocacy groups that promote digital rights and freedom of citizens. There were over 10000 people requested LQDN to refer the matter to the National Data Protection Commission (CNIL). In the two complaints, the associations reproached Google for not having a valid legal basis to process the personal data of the users of its services, particularly for ads personalization purposes. The CNIL immediately started investigating the case on 1st June 2018 and Google was found responsible for mainly two violations: lack of transparency in processing operations and no valid consent from users for obtaining user data.

2.1.1. Lack of Transparency

In terms of transparency, the restricted committee noticed that the information regarding personal data usage was not easily accessible to users. For instance, users needed to take several steps, sometimes 5 – 6 actions, to access complete information about their data collected from geo-service for the personalization purposes. In addition, users were not able to fully understand the where and how their data was

used across more than 20 services and applications associated with Google. [1]

2.1.2. Lack of valid legal basis

On the other hand, Google did not have a valid legal basis for ads personalization processing. The way which Google obtained users consent for ads personalization purposes was not valid in two ways. First, users were not sufficiently informed that their data will be applied to a range of websites, applications and services, such as Google search, Google maps, Google home, YouTube, Playstore, etc. Second, the collected consent was ambiguous. For example, when a user creates a new account, the consent was inside “More options” section, and the consent was marked as ticked by default. The users did not have a clear and specific understanding of where and what consents they agreed as registering the account. [1]

2.2. Violated Articles

Based on the above two cases, the CNIL found Google violating the below GDPR articles [3]:

- Art. 13 GDPR Information to be provided where personal data are collected from the data subject [6]
- Art. 14 GDPR Information to be provided where personal data have not been obtained from the data subject [6]
- Art. 6 GDPR Lawfulness of processing [6]
- Art. 4 nr 11 GDPR ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her [6]
- Art. 5 GDPR Principles relating to processing of personal data [6]

3. Actions

The court confirmed that the CNIL was in the right to hand down the penalty despite Google being headquartered in Ireland. The GDPR is designed to enable the home countries of companies to take the lead on enforcement efforts, but in this case, the Irish subsidiary of Google had no power of control over the other European subsidiaries nor any decision-making power over the data processing at the date of the sanction. [4]

3.1. Financial sanction

Given that the infringement observed deprived the users of essential control over consent and data processing and it has been a continuous breach of the GDPR, the CNIL decided to fine Google 50 million euros. Google appealed against the fine, but the court dismissed the appeal and the State Council issued the final decision on 21st January 2019. [4]

3.2. Google’s response

“People expect high standards of transparency and control from us,” a Google spokesman said. “We’re deeply committed to meeting those expectations and the consent requirements of the G.D.P.R. We’re studying the decision to determine our next steps.” [5]

4. Discussion

From the short and insincere response of Google, one could tell that the sanction did not do much impact on the company. After all, 50 million euros is only a peanut compared with the 134.81 billion dollars ads revenue for Google. However, as a record of the GDPR sanction fine, this case does have a symbolic effect for the other technology companies in EU.

4.1. Symbolic effects

First, tech companies would know that the GDPR enforcement process can be swift and won’t be affected easily by the geographic location of headquarters. Instead of playing with the system and trying to stall the GDPR sanctions, tech companies would better make sure that they follow all regulations carefully and stay out of trouble.

Second, 50 million euros can be a big deal to most small to medium size tech companies. If they know the fine can equal to one or multiple years of their revenue, they would probably double their procedures in obtaining user consents and how they should expose their data usage to users.

4.2. Prevention

To prevent similar incidents, tech companies could establish data compliance departments to serve as internal watchdogs, which cost much less than the GDPR sanction. In the financial tech world, financial compliance departments are well developed to guide other engineering teams navigating through sophisticated financial regulations. Unlike breaching data regulations, infringing financial regulations could face much more severe consequences, even jailtime and loss of financial licenses. Therefore, all the financial tech companies invested heavily in their own compliance department as a first line of defense against regulation violation. If tech companies in the other domains can take data regulations as seriously as financial counterparts, it would make privacy protection much easier.

References

[1] The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, *CNIL*, January 2019

<https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>

[2] Advertising revenue of Google from 2001 to 2019, *Statista*, Feb 2020

[https://www.statista.com/statistics/266249/advertising-revenue-of-google/#:~:text=In%202019%2C%20Google's%20ad%20revenue,and%20apps\)%20to%20web%20users.](https://www.statista.com/statistics/266249/advertising-revenue-of-google/#:~:text=In%202019%2C%20Google's%20ad%20revenue,and%20apps)%20to%20web%20users.)

[3] GDPR fines in accessible way

<https://github.com/lknik/gdpr/blob/master/fines/README.md>

[4] French court slaps down Google's appeal against \$57M GDPR fine, *TechCrunch*, June 2020

<https://techcrunch.com/2020/06/19/french-court-slaps-down-googles-appeal-against-57m-gdpr-fine/>

[5] Google Is Fined \$57 Million Under Europe's Data Privacy Law, *The New York Times*, Jan 2019

<https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html>

[6] General Data Protection Regulation

<https://gdpr-info.eu/>