

GDPR fine imposed upon Google: An Analysis

Ghulam Murtaza
ghulam_murtaza@brown.edu

Saim Salman
saim@brown.edu

Abstract

In this report, we give an overview and present analysis of the case brought by the National Data Protection Commission (CNIL) against Google Inc. CNIL rules that the account creation on a new android phone violated the General Data Protection Regulations (GDPR) which resulted in a financial penalty of 50 million euros on 21st January, 2019 [5].

1 Background

The GDPR (EU General Data Protection Regulation) came into effect on May 25, 2018 replacing the 1995 EU Data Protective Directive [3].

It enforces how [3]:

- Businesses can collect, use and store personal data.
- Reporting requirements for businesses to increase accountability and transparency.
- Authorizes fines on businesses that do not meet its requirements.

Due to the GDPR, businesses that process or store personal user data have started to update their businesses processes + policies to become GDPR compliant (including Google).

The importance given by Google to become GDPR compliant can be seen in their statement made in a white-paper they released in the same month of the GDPR: **"You can count on the fact that Google is committed to GDPR compliance across Google Cloud services. We are also committed to helping our customers with their GDPR compliance journey by providing robust privacy and security protections built into our services and contracts over the years."** [3]

2 GDPR Violation

2.1 Initial Complaint Report

In May 2018, after GDPR had come into force, CNIL received complaints about Google from two organizations None of

your Business (NOYB) and La Quadrature du Net (a french advocacy group) about Google's non-compliance with GDPR mainly related to Android's mobile phone set-up process.

2.2 Violation Details

The CNIL investigated the journey of a user when he creates a Google account on a new android phone and found that it violated two key breaches of the GDPR [1, 2, 5]:

- Lack of Transparency (Article 12: "Transparent information, communication and modalities for the exercise of the rights of the data subject")
- Lack of a legal basis for ads personalization processing (Article 4(11): "'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")

2.2.1 Violation 1: Lack of Transparency

Android Users found it difficult to understand the privacy policies because the information was scattered across different documents and was accessible only after multiple clicks. Furthermore, it was not clear in the document that what did the processing of the data entails, how intrusive it can potentially be. And even for users who were able to access all the documents, the language was vague + Google had used vague terms.

2.2.2 Violation 2: Lack of a legal basis for personal data processing

The forms for consent (for targeted advertisements) were neither clear and were also scattered across different document similar to Violation-1 (2.2.1) to which users were not actively

aware of the number of applications and services involved in this data processing. [5].

Also, Google also had hidden the opt-out option for personalized ads in other options which made the users passively opt-in.

2.3 Action Taken

2.3.1 One-Stop Shop

According to the Article 4 of GDPR, it provides a one stop mechanism in which the DPA (Data Protection Agency) of the nation, which houses the establishment has supervisory powers [3]. However, in case of Google, the Irish DPA (although Google had its EU entity in Ireland) wasn't given supervisory powers in place of CNIL because the main data processing and complex decision making happen in Google's US base. CNIL argued that One-Stop Shop clause didn't apply to this because [5]:

- Google never mentions Google EU as its one of the data processing entity.
- Irish DPA had not appointed any officer to overlook Google EU.
- Google said to Irish DPA that they will transfer data responsibility of EU citizens from main headquarters to EU headquarters by 31st January 2019.

Based on these arguments CNIL validated their mandate to have supervisory powers over Google in this specific case.

2.3.2 Fine

Under GDPR Data Protection Agencies (DPA) are allowed to impose a fine as high as four percent of company's annual income or twenty million euros [3], whichever is larger, as fine. CNIL fined Google 50 Million euros in fine (which was 4% of the total revenue for Google for that financial year).

2.3.3 Google's Response

“People expect high standards of transparency and control from us. We're deeply committed to meeting those expectations and the consent requirements of the GDPR. We're studying the decision to determine our next steps.”

[4] This quote from Google's spoke-person shows that they still haven't accepted their violation of GDPR. Naturally, It was expected of Google to file an appeal against the decision. The appeal will be forwarded to the French Supreme Administrative Court (Conseil d'Etat) and they might refer to European Court of Justice [5]. This appeal and its proceeding could potentially shed more light on what constitutes transparency and consent in regards to personalized and targeted ads. If the appeal is rejected Google would have to change

how they present their consent forms in accordance with the CNIL's requirements. This could have wide and long lasting implications since a lot of other companies follow Google's footsteps.

3 Discussion

Google has a full board of lawyers and advisory members on board to guide them on how to make their products GDPR compliant [3]. It implies that either Google thought their offense was in the gray area and was easily defensible in court or it was sheer carelessness which hardly would be the case. In our opinion the fine imposed on Google is justified, primarily because the breach targeted such a huge user base (more than a hundred thousand people filed a case via NOYB). Furthermore, the violation was of the core principles of data privacy and consent which makes it even more grave. Hence, the fine imposed is justified.

We believe that since companies like Google are not safe from the watchdogs of GDPR, it will make more data companies to follow the regulations put forth in the GDPR. And consequently make the entire user data processing and collection ecosystem more privacy aware.

Violation of this scale not only affects the people of EU but also everyone who has ever used an Android device or Google services (which amounts up to a very large population). Since, they might have to make their products compliant for EU population, this in turn will also make it more privacy aware for everyone around the world by extension. Since this event got a huge online traction, a lot of people translated the technical documents into simpler documents which layman can read and understand the gravity of the offense. Which in turn makes more people aware of their rights as users of these services and contribute towards a positive cycle of awareness.

Google could have easily avoided the violation if they had hired an external advisor, for example from Irish DPA. They could have had argued more solidly for additional time to roll out changes in their consent form at very least, and avoid the fine altogether.

But in lieu of this case, the authors of this report have an optimistic outlook for the future, because given Google's white paper [3] and its response it does show that giant companies are doing their due diligence to become GDPR compliant which will lead to users having more control over their privacy.

References

- [1] 2018 reform of eu data protection rules.
- [2] The cnil's restricted committee imposes a financial penalty of 50 million euros against google llc.
- [3] *General Data Protection Regulation (GDPR)*.

[4] Adam Satariano. Google is fined \$57 million under eu-
rope's data privacy law, Jan 2019.

[5] O. Tambou. France : Lessons from the first post-gdpr
fines of the cnil against google llc. 5(1):80–84, 2019.