GDPR Case Study Report: Google LLC, 2019

Colton Rusch, *Brown University* Raj Paul, *Brown University*

Abstract

On January 21st, 2019, Google LLC was fined 50 million euros by France's National Data Protection Commission (CNIL) in accordance with the General Data Protection Regulation (GDPR) [1]. Adopted in 2016 and implemented in 2018, the GDPR is an extensive regulation adopted by the European Union (EU) which concerns data protection and user privacy. In just the fourth lawsuit enforcing the GDPR towards any company [2], Google was penalized for failing to provide adequate transparency and gather sufficient consent for personal data processing related to its personalized and behavioral advertising business. In this report, we put forth the contents of the case and discuss its consequences in the broader context of data privacy, Big Tech, and legislation.

1. Background

1.1. Google LLC and Targeted Advertising

Google LLC is an American technology company that provides web services, including advertising technologies, an internet search engine, and cloud computing infrastructure. In 2019, their advertising business accounted for almost 135 billion U.S. dollars in revenue, or over 80% of their total revenue [3].

Google provides a targeted advertising service where customers can pay to place ads through Google's expansive advertisement network, which operates on Google's own web services (such as their search engine) as well as on third-party web services which opt into running ads through Google [4]. Google's advertising services are widely used due to their effectiveness, which is derived from Google's ability to collect user data and use that data to serve highly personalized advertisements, a practice also known as *targeted advertising*.

1.2. GDPR

Largely in response to the abundance of personal user data collected and used by entities such as Google, the EU passed the GDPR in order to protect natural persons with regards to the processing of their personal data. The legislation lays out what falls under its scope, constrains the definition space for relevant terms such as "personal data", "consent", and "processing", and lays out the responsibilities of data controllers and processors.

2. Violations

In May of 2018, within just a few days of GDPR's deployment, CNIL received complaints regarding Google from two privacy rights organizations: None Of Your Business (NOYB) and La Quadrature Du Net (LQDN) [1]. The complaints, filed per the mandate of over 10,000 users, claimed that Google did not have a "valid legal basis" in their processing of personal user data for personalized advertising [6].

In the official CNIL deliberation pronouncing financial sanctions unto Google, the following GDPR articles were quoted among those violated [6][7]:

- Article 5, outlining the principles regarding processing of personal data, which include lawfulness, fairness, transparency, purpose limitation, and data minimization [5]
- Article 6, outlining the conditions for lawful data processing [5]
- Article 13, outlining the information which must be provided when personal data is collected [5]
- Article 14, outlining the information which must be provided when personal data is not collected [5]

2.1. Poor Transparency

CNIL found that Google did not provide sufficiently accessible information on the personal data it collected. Likely a symptom of the immense number of services managed by Google, "essential information" including processing purposes and data storage periods was found to be "disseminated across several documents" [6]. Moreover, the committee found that several pieces of relevant information only became available to users after "5 or 6" actions [1]. In addition to poor organization, the documents themselves were found to be described in a "too generic and vague manner," as were the reported categories of data organization.

2.2. Absence of Consent

Google claimed they do not process user data for personalized ads without receiving consent, but the CNIL restricted committee reported that the consent gathered by Google for processing user data for personalized ads was invalid because it was insufficiently informed and unspecific. Users were unable to know the scope their data would be used within when agreeing to receive personalized ads, as Google failed to enumerate the applications which would show these ads, such as YouTube, Photos, Maps, etc. [6]. In this way, issues with transparency barred users from being aware of the extent of processing [1].

Moreover, Google did not collect consent with sufficient specificity. Consent was obtained through checking a box to personalize ads, however this box was pre-checked when users created a new Google account [1]. By continuing with this box checked, the user gives full consent for processing operations including ad personalization and speech recognition, but this is in violation of GDPR's requirement that consent be specific [6].

3. Outcomes

3.1. Legal Outcomes

As a result of Google's violations, CNIL imposed a fine of 50 million euros against Google on January 21, 2019.

3.2 Response From Google

In their initial response to the decision, a Google spokesman said: "People expect high standards of transparency and control from us. 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." [2]

Google appealed against the sanction levied by CNIL, but on June 19, 2020, CNIL's decision was upheld by the French Council of State, who found that the violations reported by CNIL were consistent and the imposed fine was not disproportionate relative to the severity of the violations [8].

4. Discussion

This case remains an especially significant one in the history of data privacy enforcement for its magnitude and timeline. The fine issued to Google remains one of the largest filed towards any tech company as part of GDPR's enforcement, and this case set an enormous precedent for the gravity of the GDPR. This fine of 50 million euros was the largest sum allowed by the GDPR, which limits fines to 4% of a company's annual earnings.

We find the fine imposed to be appropriate with the circumstances of the case, as issuing the maximum amount matches the severity of such blatant negligence in transparency and consent on Google's part. As Google's services and user bases span the globe, the violations affected far more users than those who appealed to CNIL through NOYB and LQDN — in fact, it affected each individual of Google services. We found these legal proceedings to be ultimately successful as they ran through an appropriate body (CNIL), collected the fines charged, and resulted in Google improving their efforts to obtain user consent and provide transparency.

4.1. Prevention, for this case and future

In this case, Google could have prevented violating the GDPR by (1) ensuring that essential data privacy information was easily accessible to users and well-articulated as well as (2) vetting the presentation of and methods used while gathering user consent for data processing. To generalize, it is of utmost importance for companies to be transparent and thorough when describing the personal data they gather on their users and the way that they use this data. Users can only consent when they are sufficiently informed about the specific terms of their consent; the responsibility falls on the companies to provide a means for users to understand the full scope of their consent.

In terms of actionable steps that companies may take to prevent similar issues in the future: having an internal team devoted to auditing and vetting the company's data privacy policies and the way these policies are presented to users could help companies avoid making violations in the first place. It is likely that the expenses required to do so would amount to much less than what potential GDPR fines or losses due to bad publicity would.

Google's errors in this case, while clearly in violation of the law, are at least understandable; many companies have opted to cut corners on data privacy transparency throughout their operations, meaning that they're left unprepared when regulations crack down on their privacy practices. It's unlikely that Google had forgone preparations for the GDPR's implementation entirely. Instead, they likely missed many potential violations due the scope of their businesses and the sheer volume of processes to audit for compliance. While not all companies possess the similar scale and complexity of Google, it's not hard to imagine that, for many companies, it's hard to cover everything when tackling GDPR compliance, especially when ensuring compliance retroactively.

References

[1] https://www.bbc.com/news/technology-46944696

[2] https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html

[3] https://abc.xyz/investor/static/pdf/2019Q4_alphabet_earnings_release.pdf

[4] https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html

[5] https://gdpr-info.eu/

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

[7] https://www.enforcementtracker.com/

[8] https://www.conseil-etat.fr/actualites/actualites/rgpd-le-conseil-d-etat-rejette-le-recours-dirige-contre-la-sanction-de-50-millions-d-euros-infligee-a-google-par-la-cnil