

**FIRST MAJOR BREACH OF THE GDPR:
FRANCE FINED GOOGLE €50.000.000**

Murat Volkan Dülger*

€50.000.000 that fined to Google by the French authorities in consequence of the breach of the GDPR demonstrates the GDPR's quick entrance to the field, which has been in force for only less than a year. Thereby, the first major breach since the GDPR has come into force has been occurred and the administrative fine regulated under the GDPR has been imposed thereafter.

As “*personal data*” changed dimension over time, the need to modernise the principles recognised in Directive 95/46/EC (“Data Protection Directive”) and to reform this area in order to ensure effective protection to the personal rights has emerged. To that end, European Parliament accepted the GDPR on the 24 May 2016, which replaces the Data Protection Directive. Additionally, the GDPR provided for a two year-transitional period after its adoption and it became applicable on 25 May 2018. Thus, the GDPR is newly applicable.

The GDPR is the most up-to-date regulation with the strictest conditions, and the EU Member States have been preparing themselves to these conditions since its text was published. The most distinct and worrisome characteristics of the GDPR were its whole and direct applicability, expanded territorial scope and high administrative fines regulated therein. Indeed, fining a company like Google with such high amount reveals that the worrisome were accurate.

It should be born in mind that the GDPR's territorial scope is broader than the EU borders and it is also applicable to data processing concerning the citizens or residents of the EU; hence, the GDPR is also of a great importance for Turkey. Thus, the companies that resident in Turkey but operate internationally must be careful in that regard and act for complying with the provisions of the GDPR which provides a greater protection than the Law no. 6698 (“Turkish Data Protection Law”).

The companies which are aware of the above-mentioned characteristic of the GDPR want to carry out compliance projects in accordance with both the Turkish Data Protection Law and the GDPR. Therefore, the companies that in the scope of the GDPR must pay attention to this matter.

1. The Administrative Fine Imposed on Google by France

a. Investigation Process Initiated on Google

The investigation concerning Google was initiated by two privacy defenders upon the complaints made on 25-28 May 2018. Both organisations claimed that Google did not have a valid legal basis for processing personal data and this was done especially in order to personalise advertising. The top data protection authority of France, *CNIL (Commission Nationale de l'Informatique et des Libertés)* commenced investigation upon the complaints.

* PhD., L.L.M, Assoc. Prof. of Criminal Law and IT Law, volkan.dulger@dulger.av.tr

It was noted that aforementioned privacy defenders also brought complaints in other EU Member States against Facebook and its subsidiaries, photograph sharing application Instagram and messaging service WhatsApp. Hence, there is a possibility that high administrative fines would be imposed on these companies, if an investigation is initiated against them and a data breach by them is determined.

In the wake of the investigation, CNIL made a statement on its investigation and findings.¹ CNIL noted that during this investigation, the data protection authorities in other Member States was frequently contacted and information exchange was carried out. Furthermore, it stated that, according to the new practice, like all Member State protection authorities, it is entitled to decide on Google's practices.

CNIL mentioned that it has conducted an online control in September, for the purposes of searching about the complaints. It declared the aim of this control as determining a user's journey and the documents that could be reached by creating a Google account. Thus, Google's compliance with the French national laws regarding personal data processing and with the GDPR could be verified.

Google made some alterations in order to comply with the EU rules. Nonetheless, CNIL stated that the observed breaches are still based on extensive data, therefore information regarding the users' private lives could come up as a result of limitless possible combination. Within this scope, Google could not explain how the personal data of the users was collected and what was it composed of.

Whereas, pursuant to the GDPR and other EU data protection laws, a technology company must be able to provide the users with all personal data collected. Moreover, simple, clear and purpose-specific means for obtaining consent from the users in relation to processing of their personal data must be presented.

In response to this, Google expressed that their next step would be analysing the decision, and it added that: *"People expect high standards of transparency and control from us. We are deeply committed to meeting those expectations and the consent requirements of the GDPR."*

b. Deficiencies of Google that determined through the investigation

Ultimately, about Google, CNIL determined deficiencies with regard to two main obligations regulated under the GDPR:

i. Obligation to inform

According to CNIL, information provided by Google is not easily accessible. It is determined that important information, inter alia, the purposes of data processing, duration of data storage and data categories that used to personalise advertising, is not included in the information that chosen by the company to be shown at the first stage. This information is spread between various options and connections. Withal, a setting must be activated in order to read the

¹ See CNIL's full statement on <https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la>.

additional information. The relevant documents are only being accessed after several steps and five or six actions. For instance, a user who wants to obtain information with regard to collection of personal data for personalised advertising must go through the aforesaid steps. Furthermore, the limited training given with respect to relevant information did not find to be clear and understandable.

Therefore, CNIL expressed that the users could not understand the scope of the actions operated by Google. Nonetheless, it is of the opinion that massive data processing is conducted by virtue of these actions which are defined in an unspecific manner and very vaguely. In other respects, it is detected that duration of storage in relation to some data is not specified within the limited information given.

The GDPR regulates the obligation to inform both separately and under the transparency principle. Any information and communication concerning data processing must be easily accessible and understandable for the data subject and its language must be clear and plain.²

ii. Transparency and clarity

CNIL addressed the deficiencies with regard to transparency and clarity, especially within the scope of personalised advertising. It is of the opinion that, due to the detected deficiencies, Google does not base its practices in that regard on a legal ground.

Google obtains the consent of the users for personalised advertising and acts accordingly. However, CNIL considers this consent to be invalid. Firstly, it touched on that the above-mentioned obligation to inform is also applicable in this respect. It stated that the users are not informed sufficiently regarding their consent and they are not allowed to perceive the dimension of the information used. To illustrate, it is not possible to be informed of the services, websites and applications like Google Search, Google Play, Google Home, Google Maps, Google Play Store, Google Photo at the privatisation of the advertising segment. However, extensive data is processed and combined therein.

CNIL further bases its opinion on the invalidity of the consent on the fact that it is not specific, explicit and transparent. Even though it acknowledges the feasibility of changing some of the parameters relevant to the account by clicking “more options” while creating an account, it stated that this is not in accordance with the GDPR. It mentioned that default options must also be checked beforehand. Furthermore, it called attention to the fact that Google take the users’ statements such as “I agree to the Terms of Service of Google” and “I accept that my information is used as explained in detail above”, prior to the creation of the account. However, a manner like this induces a “block consent” for all purposes that Google bases its personal data processing on, including personalisation of the advertisements and voice recognition.

However, GDPR requires a consent given for a specific purpose and given separately for each purpose, as it is necessitated by the principle of purpose limitation, i.e. the requirement that any collecting and processing of personal data must be done for a specific and explicit purpose. In

² **Murat Volkan Dülger**, *Kişisel Verilerin Korunması Hukuku*, İstanbul, Hukuk Akademisi, 2019, s. 115.

order to comply with this principle, the data to be processed and the purposes of processing such data must be determined. The determined purpose must be clear to the data subject.³

Moreover, the transparency principle is introduced with the GDPR, as distinct from the Data Protection Directive. In order to ensure compliance with this principle, the data subject must be informed on the identity of the data controller, the purposes, means, risks and rules of data processing and its rights regarding the processing activities.⁴ Hence, it is possible to conclude that the transparency principle is strongly connected with the obligation to inform; thus, a personal data processing that based on insufficient and limited informing would also be considered to be non-transparent.

c. Sanction Decision Regarding Google

CNIL fined Google a record €50.000.000 for failing to comply with the aforesaid terms of the GDPR. This decision also constitutes the first fine of the GDPR regime imposed by CNIL, which provides for high administrative fines. CNIL stated that the imposed fine is proportionate to the severity of violating the obligation to inform and transparency and acting in defiance of the conditions of consent regulated under the GDPR.

Notwithstanding some precautions taken by Google, the determined deficiencies suffice to uncover the users' privacy and they deprive them of the main safeguard. CNIL addressed that Google users must have adequate control over their data, must be informed sufficiently and must be in a position to give a valid consent.

Besides, it expressed that this breach is not limited to a certain time period, to the contrary, it is of a continuous nature.

d. Reactions Following the Decision

The most notable aspect of this decision is the determination of a major data breach under the GDPR. Additionally, it concerned the largest company of the US, Google, and it ruled for a huge amount of administrative fine. Thus, this decision was interpreted by a broad range of people.

Max Schrems, the head of Noyb (None of Your Business)⁵, stated that they are pleased that European data protection authorities are using the opportunities which are brought by the GDPR for the purposes of punishing the breaches. According to his opinion, it is crucial that the decision declared that a mere statement by the competent authorities that claim compliance with the regulation is not sufficient for demonstrating compliance.

In that regard, an important rule recognised by the GDPR was touched upon. "*The principle of accountability*" is adopted with the GDPR, which is not included in the Law no. 6698 and many

³ Dülger, s. 117.

⁴ Dülger, s. 115.

⁵ Noyb is an organisation established following the GDPR which conducts projects on privacy breaches.

other national laws. Pursuant to this principle, the data controller shall be responsible for, and must be able to demonstrate compliance with the personal data processing principles.⁶

Estelle Massé, a data protection expert from Access Now⁷ made similar statements and drew attention to the application of the GDPR. It interpreted this decision as the first major sign showing the willingness of Europe to apply the GDPR. Likewise, she called attention to the analogous practices of the companies and mentioned that other technology companies will also face fines.

Marc Rotenberg, the general manager of the Electronic Privacy Information Center (EPIC), complained about the delay by the Federal Trade Commission (FTC)⁸ to take an action against the technology companies.

With regard to the imposed administrative fine, there were criticisms arguing that the fine is low, especially on the side of the consumer rights defenders. It was also complained that France is not progressed enough. Indeed, La Quadrature du Net, which is one of the complainants against Google, stated that the imposed fine is extremely low by comparison with Google's annual return.

Conclusion

This decision has a great importance as the sanction decision was given as a result of the application of the GDPR. As the qualification of the determined breaches and the basic principles which the breaches are in relation with were explained above, I prefer to lay emphasis on the fact that only one European data protection authority has applied the GDPR, confirmed the violation and ruled for administrative fine.

As mentioned above, GDPR was accepted on 24 May 2016 and it provided for strict conditions with respect to personal data protection and privacy, and for two year-transitional period. During this two-year-period, implementation projects was conducted to ensure compliance with the GDPR, especially by the companies located in the EU. This is particularly an important obligation for technology companies that use extensive amount of data. Indeed, even though Google carried out numerous updates, these updates was not found adequate in order to ensure compliance with the GDPR.

This implies that EU Member States would not make concessions to the application of the GDPR. Furthermore, despite it was found insufficient by some communities, the amount of the imposed administrative fine must give rise to thoughts of the data controllers. Hence, it must be understood that the provisions of the GDPR would be strictly applied throughout an investigation initiated upon a complaint, also a great emphasis would be put on whether the basic principles were violated or not. In case of determining a violation, the data protection

⁶ Dülger, s. 139.

⁷ "Access Now" is an organisation that defends and extends the digital rights of users at risk around the world.

⁸ Federal Trade Commission is Washington's top privacy and security agency.

authorities would not abstain from imposing sanctions, and the administrative fine would be of a dissuasive nature.

Therefore, as stressed above, the companies that resident in Turkey but operate internationally must be careful and refrain from a perspective suggesting that the GDPR would not be applicable in their cases since Turkey is not a member of the EU. The GDPR is not a conventional international regulation and its territorial scope is broader than the EU borders. Hence, it is evident that a country like Turkey which carries on extensive economic and commercial business with the EU Member States would be affected by the GDPR. Thus, I recommend such companies not to be limited to the Law no. 6698 and take steps in order to become accordant with the GDPR which provides for stricter conditions.