Recent Developments on Personal Data Protection in Turkey (April – May 2019): Microsoft's Data Breach, Facebook's Violation, and More

Recent Developments on Personal Data Protection in Turkey (April – May 2019): Microsoft's Data Breach, Facebook's Violation, and More

Article by Ertuğrul Can Canbolat, Baran Can Yıldırım, and S. İrem Akın

Introduction

Turkish personal data protection practice presented some noteworthy developments in April and May 2019 as the Turkish Data Protection Authority ("**DPA**") published through its website several summaries of its recent decisions shedding light on issues such as "*legitimate interest of the data processor*", "*explicit consent*", "*obligation to inform*", and "*data security*". The DPA also published a new guideline on the "*Personal Data Processing Inventory*".

Particularly, the DPA announced that Microsoft notified the DPA about a data breach occurred in Microsoft's systems. Microsoft was not fined as it reportedly took necessary security measures to prevent further breaches. On the other hand, the DPA fined Facebook on the grounds that Facebook failed to notify the DPA about an API bug, which led to unauthorized access by third-party applications to the Facebook users' photos and Facebook's security measures are not sufficient to prevent such breach, and to detect what exactly was leaked to whom.

We will explain and discuss throughout this article the decisions published by the DPA dealing with the abovementioned issues as well as the new guideline.

Microsoft's Data Breach Notification

On 10.05.2019, the DPA announced that Microsoft Corporation ("**Microsoft**") notified on 08.05.2019 the DPA about a data breach occurred in their system[1].

Microsoft reported that the ID information of a call support manager working for one of Microsoft's services providers has unauthorizedly been obtained by the third parties.

Microsoft determined that the said manager was contrary to Microsoft Policy shared his/her account's login information with 13 support representatives. Microsoft reported that these support representatives may have been a victim of an e-commerce fraud, which may then have led to the notified data breach. However, Microsoft also stated that one or more of the said support representatives may have been responsible for the breach.

As a result, third parties were able to partly reach to Microsoft users' e-mail accounts between

01.01.2019 – 28.03.2019. Microsoft stated that the third parties may have viewed or accessed the e-mail addresses, subjects of the e-mails, recipients of the sent e-mails. However, the content or the attachments of the said e-mails, except for a "*very small part*", were not accessed. Microsoft immediately unauthorized the leaked login information of the manager it became aware of the breach. It was reported that an estimate of 1,820 people in Turkey may have been affected due the unlawful access.

Microsoft further warned that phishing attacks may occur in the future on the affected users. The DPA still continues its examination on the incident, the DPA decided to announce the data breach on its website right after the filed notification probably due to its importance and possible effects on the Microsoft users.

TRY 1,65m Fine on Facebook

The summary of the DPA's decision dated 11.04.2019 and numbered 2019/104[2] deals with the results of the investigation initiated *ex officio* by the DPA against Facebook. According to the summary of the decision, Facebook was fined 1,650,000 TRY in total.

The DPA published the amount of the fine imposed on a company for the first time, which is considered as a signal emphasizing the importance of compliance with the data protection rules stipulated under the Data Protection Law.

The DPA indicated that its investigation regarding Facebook was initiated due to a software error occurred at the end of 2018 announced by the Facebook's Engineering Manager Tomer Bar. According to the DPA, the announcement entitled "*Notifying our Developer Ecosystem about a Photo API Bug*" indicates that Facebook breached several data protection rules.

In this respect, it is determined that the concerned API bug took place between 13 – 25 September 2018 and may have affected about 300,000 users in Turkey. The DPA also stated that, due to the API bug, the third-party applications were able to reach to the user photos for which access was not allowed by the owners, and that this situation constituted a breach of the following data protection principles: "*being in conformity with the law and good faith*" and "*being relevant, limited and proportionate with the purposes for which data are processed*". Facebook was not able to determine whether the third-party applications accessed the photos that are not allowed by the owners and the DPA deemed this as another breach of the data controller's obligations regarding data security.

In addition, the DPA determined that during the process of giving permission to third-party applications, the consent obtained by Facebook from users for the access to their friends' information and other information cannot be regarded as an "*explicit consent*" under the Data Protection Law. It is reminded by the DPA that explicit consent should be given with free will and that it should not be put forward as a precondition for the provision of a product or service or to benefit from the service. Therefore, it is decided that Facebook breached the principle of "*being in conformity with the law and good faith*".

Lastly, Facebook only informed the users in December 2018 and did not inform the DPA at all, even though the API bug occurred in September 2018, which was determined as another violation by the TCA.

In the light of these findings, the DPA imposed an administrative fine of 1,100,000 TRY as Facebook failed to take all necessary technical and organizational measures, and of 550,000 TRY as Facebook did not fulfill its obligations regarding the data breach notification.

Data Processing Without Explicit Consent: Legitimate Interest Condition

In the summary of the DPA's decision dated 25.03.2019 and numbered 2019/78[3], the DPA reminded that personal data can be processed without the explicit consent of the data subject in cases where the processing is necessary for the legitimate interests of the concerned data controller. The summary of the DPA's decision is of particular importance as it draws the framework as to how the legitimate interest of a data controller should be assessed in processing personal data without the explicit consent of the concerned data subjects.

In order for the personal data to be processed without the explicit consent of the data subject, such process must be based on one of the legal grounds set forth in Article 5 of the Data Protection Law. Legitimate interest of the data controller is given as one of these legal grounds. In this regard, a data controller may process without seeking the explicit consent o the data subject where it is mandatory for the legitimate interests of the controlled, provided that this processing does not violate the fundamental rights and freedoms of the data subject.

In the light of this decision, it is understood that a company operating under the Distribution License within the scope of the Petroleum Market Law has applied to the DPA and requested permission to processes personal data regarding the license plate and fuel type of the data subjects' cars without obtaining explicit consent with a view to prevent incorrect fuel filling. By processing the data subjects' license plate and fuel type of the cars, the company aims to determine automatically which type of fuel is suitable for each vehicle and prevent possible damages that may occur due to incorrect filling.

The DPA first determined that the processing activities of the firm are originally based on the condition of "*being necessary for compliance with a legal obligation which the controller is subject to*" due the Energy Market Regulatory Authority's legal requirements. The DPA established that as the processing personal data for another purpose constitutes a new processing activity, this new processing activity shall also be based on another legal ground for processing.

As a result of the examination carried out; it has been determined that the implementation of the new processing may eliminate the problems that both consumers and the companies operating in this market might face and may further prevent the losses that might occur in the brand value and service quality. In light of these findings, it is decided that; (**i**) the new processing activity may be realized based on legal condition of "*being necessary for the legitimate interests of the data controller,*

provided that the fundamental rights and freedoms of the data subject are not harmed" and (**ii**) there is no legal obstacle in implementing the new project without obtaining the explicit consent of the data subjects provided that the obligation to inform is fulfilled in a way that is reachable and visible by the data subjects and the processed personal data is not be used for other purposes.

It is understood that the DPA will consider the following transparent elements that can be accounted for by the data controller in assessing whether there exists legitimate interest in every individual case such as

- "*whether the concerned benefit is arising from the processing affects many people*"
- "*whether it solely serves to the purpose of profit or economic benefit of the data controller*"
- "*whether it simplifies a business process or manner (e.g. not in a way that it will only affect a single unit or a small number of employees in the firm but affects the whole entity)*"

Employment Processes: Obligation to Inform and Explicit Consent

In the summary of the DPA's decision dated 26.07.2018 and numbered 2018/90[4], the DPA has reminded that the processes for obligation to inform and obtaining the explicit consent of the data subjects shall be carried out separately.

The DPA determined that a company required its employee candidates to register to an online platform for the submission of their job applications. In the registration process, the company required the employee candidates to check a single *checkbox*, which indicates both (**i**) that the Privacy Policy of the company is read by the candidate, and (**ii**) that the candidate has given their explicit consent to the processing of their personal data by the company. Therefore, it is understood that the company processes the candidate's personal data based on their explicit consent.

However, as Article 5(1)(f) of the Communiqué on Principles and Procedures for Fulfillment of Obligation to Inform sets forth; where the data processing activities are based on explicit consent, the process for the obligation to inform and obtaining explicit consent must be carried out separately by the data controllers. It is emphasized that the main purpose of the obligation to inform, which may be fulfilled through publishing privacy policies, is to ensure that the concerned data subject is informed about the processing of their personal data whereas obtaining explicit consent of the data subject serves as the legal ground for a processing. In this regard, it is concluded that fulfilling these two different obligations through the same action (by checking a single *checkbox*) is contrary to Data Protection Law and therefore these two processes shall be separated by the concerned data controller.

The Failure to Fulfill the DPA's Decisions and Its Consequences

In the summary of the DPA's decision dated 16.10.2018 and numbered 2018/118[5], the DPA emphasized that the data controllers are obliged to fulfill the orders of the DPA's decisions within a 30-day period.

Pursuant to the Data Protection Law, any person making a request regarding their personal data should first apply to the data controller. Where the application is (**i**) rejected, (**ii**) replied insufficiently, or (**iii**) not replied in due time, the data subject can then file a complaint to the DPA. The concerned data controller shall take the necessary actions stated in the DPA's decisions "*as soon as possible and in thirty days at most*" according to Article 15 of the Data Protection Law.

It was determined by the DPA that the thirty-day period has been exceeded in the present case and the necessary actions have not been taken by the concerned data controller, which was a public institution. The DPA decided to imply administrative measures on the concerned data controller pursuant to Article 18/3 of the Data Protection Law as (**i**) the necessary measures were not taken by the concerned data controller within the thirty-day period and (**ii**) some of the requirements of the DPA decisions were not fulfilled by the data controller. It is further understood that the public officials (as the employees of the public institution data controller) will be subject to disciplinary penalties through the reference to Article 18/3 of the Data Protection Law.

The DPA Published the Guidelines on Personal Data Processing Inventory

The DPA published on 30.04.2019 the *Guidelines on Personal Data Processing Inventory* on its website[6]. With the amendment in 28.04.2019 to *Regulation on Data Controller's Registry,* preparation of a Personal Data Processing Inventory became an obligation for all the data controllers who are obliged to register to the *Data Controller's Registry*. In line with this amendment, the DPA published the *Guidelines on Personal Data Processing Inventory*.

The main reason for the obligation to prepare an inventory was stated as "*ensuring compliance with the Data Protection Law in all of the processes related to the activities of the data controllers*". It is also indicated that the inventory will enable the data controllers to self-audit themselves by creating an auto-control mechanism.

It is also emphasized that the inventory will be used in the following processes: (**i**) registration to the Data Controller's Registry, (**ii**) fulfilling the obligation to inform, (**iii**) answering the applications of the data subjects and (**iv**) determining the scope of the explicit consent.

Conclusion

The DPA keeps developing its precedent in light of the sectors' needs. The DPA also demonstrated by its Facebook decision that it started to take more serious steps towards any non-compliance with the Data Protection Law. Microsoft's announcement reveals that even the biggest tech giants may be subject to data breaches unless adequate compliance and security measures are taken both internally and with regards to the third-party service providers as well as their employees.

The DPA is shedding light on the vague rules in the area of data protection. As the case law grows and is presented to the sectors' attention, it is expected that the DPA will be stricter in terms of any incompliance with the data protection rules.

Footnotes

1. https://www.kvkk.gov.tr/Icerik/5451/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Microsoft-Corporation

2. https://www.kvkk.gov.tr/Icerik/5450/2019-104

3. https://kvkk.gov.tr/Icerik/5434/2019-78

4. https://kvkk.gov.tr/Icerik/5420/-Veri-sorumlusu-tarafindan-aydinlatma-yukumlulugu-ve-acik-riza-onayi-alinmasi-sureclerinin-ayri-ayri-yerine-getirilmesi-gerektigi-ile-ilgili-Kisisel-Verileri-Koruma-Kurulunun-26-07-2018-tarihli-ve-2018-90-sayili-Karar-Ozeti

5. https://kvkk.gov.tr/Icerik/5422/-Kurul-Kararinin-gereginin-suresi-icinde-yerine-getirilmemesi-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-16-10-2018-tarihli-ve-2018-118-sayili-Karari

6. https://www.kvkk.gov.tr/Icerik/5445/Kisisel-Veri-Isleme-Envanteri-Hazirlama-Rehberi-Kurum-Internet-Sayfasinda-Yayinlanmistir