
Turkish Data Protection Watchdog: If You Use Gmail, You Are Transferring Personal Data Abroad

A Brief Overview of the Recent Developments Regarding Personal Data Protection in Turkey (May – September 2019)

Article by Ertuğrul Can Canbolat, Baran Can Yıldırım, İrem Akın

Introduction

The Turkish Personal Data Protection Authority ("**DPA**") recently released a number of decisions that are of significance in various terms such as abuse of right to process personal data and explicit consent.

Unlike the Turkish Competition Authority, the DPA is not obliged to publish its decisions, which in fact came under criticism on the ground that it contradicts with the principle of transparency. In considering the range of subjects and sectors that the DPA's have dealt with so far in its published decisions, we understand that the DPA chooses carefully which of its decision should be published with a view to address publicly as many sectors as possible.

Throughout this article, we will discuss these recently published decisions.

Using Company E-mail Addresses via Gmail is Transfer of Personal Data Abroad

The DPA ruled on 31.05.2019 that buying services from data controllers or data processors whose data centers (*servers*) are located abroad is a transfer of personal data abroad within the scope of the Personal Data Protection Law ("**DP Law**") (31.05.2019; 2019/157)[\[1\]](#).

Upon an application submitted regarding whether the e-mail addresses provided by "*Zimbra*", which provides free corporate e-mail services, could be used over Gmail with the same extension. After the examination, the sent and received e-mails using the Gmail infrastructure are kept in the servers located in different countries are considered as transfer of personal data abroad.

Here, it should be noted that, according to Article 9 of the DP Law, transfer of personal data abroad may only be carried out under the circumstances listed below:

- relying on one of the data processing conditions set forth in the DP Law **and**
- the foreign country to whom personal data will be transferred has an adequate level of protection (the relevant country is regarded as "*safe country*") **or** in case there is no adequate protection in the concerned country, if the concerned data controllers (in Turkey and abroad) submit their written commitments and the DPA has given permission to such transfer.

However, the DPA has not yet announced the list of the countries with an adequate level of protection.

In this regard, transfer of personal data abroad which does not fulfill the requirements stated above may be lawfully carried out *only if* data subjects' explicit consent (see [Guidelines On Explicit Consent](#)) is obtained. Therefore, while determining whether a country is among the "safe countries"; the legislation and "[Criteria for Determining the Countries with Adequate Protection](#)" published by the DPA should be carefully evaluated in accordance with the present regulations to avoid potential risks while transferring personal data abroad.

Sending Excessing Number of SMSs on the Same Subject Was Considered as an Abuse of Right

The DPA ruled that SMSs to a data subject on different dates and multiple times on the same subject might constitute "*abuse of the right of the data controller*", even when the said data controller has lawful processing basis (31.05.2019; 2019/159)[2].

A data subject, who received many SMSs without his explicit consent from an asset management company first applied to the concerned company and then brought his case before the DPA. Upon the examination, the DPA decided that the Company has the right to send out those SMSs as it is "*mandatory for the establishment, exercise or protection of a right*" [3] since these SMSs were sent with a view to remind the debtor (data subject) about his legal risks and rights attached to his debt. Therefore, the DPA ruled that it was not necessary for the Company to obtain the explicit consent of the data subject. However, the DPA also considered the frequency of these SMSs and determined that sending same content multiple times on different dates constitutes an abuse of right and decided to impose an administrative fine of TRY 20,000 on the concerned data controller.

Hereby, the DPA reminded that the processing the personal by relying on one of the legal basis stated under the DP Law is not enough *per se* to comply with the data protection rules but also all data processing activities should be carried out in accordance with the purpose of processing and *bona fide* rules.

Commercial Electronic Messages That Include Advertisements Sent Without Explicit Consent May Be Unlawful

All data controllers are under the obligation "*to prevent the unlawful processing of personal data*" and a data processing activity which lacks at least one of the data processing conditions mentioned in Articles 5 and 6 is a breach of the DP Law.

In this decision (31.05.2019; 2019/162)[4], a data subject who had been receiving SMS advertisings from a data controller, submitted a complaint to the DPA after not being able to receive a response from the company. Here, an administrative fine of TRY 50,000 was imposed on the data controller as it was sending out the SMSs without relying on any of the data processing conditions.

In another recent decision (08.07.2019; 2019/204)[5], an employee of a company sent commercial SMSs to a data subject. Interestingly, it was observed that the relevant employee reached to the telephone number of the relevant data subject through his former company which operated in the same field as the new data controller company where the concerned employee currently works. As a result, it was concluded that the processing was not relying on any of the data processing conditions and therefore an administrative fine of TRY 75,000 was imposed. Also, regarding the allegations about the transfer personal data to the new company, the DPA decided to inform the relevant employee about Article 136 of the Turkish Criminal Law which foresees imprisonment up to for years for the cases where data is unlawfully spread, acquired or delivered to another person through illegal means.

The Use of Hand-Palm Reading System by The Gyms Was Considered as Processing of Special Categories of Personal Data

The DPA published two decisions (25.03.2019; 2019/81 and 31.05.2019; 2019/165)[6] regarding the activities of the gyms that had been using *hand-palm reading systems* to control the entrance/exit of their members. Upon the examination of the notices and complaints received concerning such applications, the DPA reached to several important conclusions.

First, the use of hand-palm reading system was regarded as processing of biometric data. Therefore, it was stated the concerned activity should be evaluated within the scope of the processing of special categories of personal data. Even though it was observed that the relevant data controllers obtained explicit consent of the data subjects for such application, this was found unlawful as the explicit consent was obtained as a precondition of provision of a service. As such, people who did not want to give explicit consent were not admitted to the membership. In accordance, the DPA concluded that compulsory "*hand and fingerprint reading system*" does not comply with the principle of proportionality since there are many alternatives to this practice.

In light of above, the DPA decided that (i) the consent obtained from the members violated the DP Law, (ii) adequate technical and administrative measures were not taken by the gyms, (iii) an alternative way to this practice must be found and processing biometric data must be immediately stopped, (iv) the data obtained so far containing hand, finger and palm print must be destroyed in accordance with the legislation and (v) the third parties, to whom such personal data was transferred, must be notified of the destruction and (vi) an administrative fine was imposed on the relevant gyms.

Contacting with The Debtor's Family Was Found Against the DP Law

A lawyer was found in violation of the DP Law through a decision (31.05.2019; 2019/166)[7] since he/she sent a SMS containing personal data to one of the debtor's family members instead of the debtor. As a result of this practice, lawyer resulted faced an administrative fine of TRY 50,000.

Here, the DPA concluded the lawyer violated the DP Law as a result of two separate data processing

activities tied to a single action which are; (i) sending the personal information of the data subject to the complainant's (who is a relative of the data controller) telephone number and (ii) processing the telephone number without relying on any of the processing conditions set out in the DP Law.

Announcing the Exam Results Publicly by a University Considered as a Violation of The DP Law

Another recent decision (01.07.2019; 2019/188)[8] concerns Mimar Sinan Fine Arts University ("University") – a public university in Istanbul, and its practice of announcing the results of the exams publicly on the Internet.

After its examination, the DPA found that the exam results of the students were announced publicly by the University and the results were kept available online to third parties even after years. Also, this practice of the University led the exam results to be accessed easily when searched online through search engines for many years.

Upon examination, it was found that each university has the authority to decide on the way of announcing the results and on how long they would be accessible. Accordingly, the DPA decided that the exam results to be easily accessed by third parties without relying on any processing conditions constitutes a violation of the DP Law. It was further decided that the way the exam results are announced should be revised by the University in a way that only the individuals who took the exam should have access to their own results. Therefore, the University was instructed to revise its practice accordingly.

Conclusion

Through these publications, the DPA did not only expand its precedent but also provided a wider and more in-depth guide to the data controllers in Turkey. Also, since the decisions concern different professions and sectors, it helps to attract more individuals and companies.

[1] <https://www.kvkk.gov.tr/Icerik/5493/2019-157>

[2] <https://www.kvkk.gov.tr/Icerik/5494/2019-159>

[3] Article 5/2(e) of the Personal Data Protection Law.

[4] <https://www.kvkk.gov.tr/Icerik/5495/2019-162>

[5] <https://www.kvkk.gov.tr/Icerik/5517/2019-204>

[6] <https://www.kvkk.gov.tr/Icerik/5496/2019-81-165>

[7] <https://www.kvkk.gov.tr/Icerik/5497/2019-166>

[8] <https://www.kvkk.gov.tr/Icerik/5506/2019-188>