Turkish Data Protection Authority's New Decisions Published on July 17, 2019

Authors: Gönenç Gürkaynak, Esq., Ceren Yıldız, Burak Yeşilaltay and Ekin Ince, ELIG Gürkaynak Attorneys-at-Law

Turkish Personal Data Protection Board ("Board") published five (5) new decision summaries on the Data Protection Authority's ("DPA") website on July 17, 2019.

I. Use of Private E-Mail Services for Corporate E-Mail Addresses (Board's Decision 2019/157)

Board's decision of May 31, 2019 with number 2019/157 has been rendered in response to a request from a data controller for Board's guidance on the matter of whether a private e-mail service, provided by a foreign company, can be used for corporate e-mail addresses obtained through an open source e-mail service.

The Board stated that the e-mail messages sent or received through the relevant e-mail addresses using the relevant private e-mail service's infrastructure might be stored in data centers located in different parts of the world and therefore, personal data would be deemed to be transferred abroad. Accordingly, the Board concluded that data controllers willing to use the relevant private services shall do so in compliance with the rules on transfer of personal data abroad under Turkish data protection laws (Article 9 of Law No. 6698 on Protection of Personal Data ("DPL")).

Moreover, the Board stated that storage services obtained through data controllers/data processors whose servers are located abroad shall also be in compliance with Article 9 of DPL.

II. Sending Commercial Electronic Communications without Data Subject's Explicit Consent (Board's Decision 2019/162)

Board's decision of May 31, 2019 with number 2019/162 concerns a complaint filed by a data subject on the grounds that commercial electronic communications has been sent to his/her mobile phone number without his/her explicit consent.

The individual claimed that (i) he/she does not know from where and how his/her personal data has been obtained, (ii) he/she did not explicitly consent to receiving such communications and (iii) he/she contacted the data controller to request information but did not receive a response from the data controller in the legal time period.

The data subject requested the following information from the Board: (i) whether data controller has his/her explicit consent to send commercial electronic communications, (ii) whether his/her personal data has been processed and if yes, for which purposes, (iii) to whom his/her personal data has been transferred in Turkey, (iv) whether his/her personal data has been transferred abroad, and if yes to whom, (v) whether data controller is aware of the commercial electronic communications that are sent to him/her.

The Board evaluated the complaint and concluded that sending commercial electronic communications to the data subject's mobile phone number is a data processing activity and in the case at hand, such processing is not based on any of the legal reasons listed in DPL. As a result, the Board imposed an administrative fine of TL 50,000 on the data controller for failing to take technical and administrative measures in order to ensure an adequate level of security to safeguard and prevent unlawful processing of and access to personal data.

III. Processing of Biometric Personal Data by Fitness Centers (Board's Decisions 2019/81, 2019/165)

Board's decisions of March 25, 2019 with number 2019/81 and of May 31, 2019 with number 2019/165 relate to processing of biometric personal data by two different data controllers, which are both operating fitness centers, during entrances and exits of their members. Data subjects made multiple notifications to the Board indicating their concerns regarding safe storage of their biometric information including hand and palm prints as well as practices as such public display of their photos and hour of their last visit at the facilities on television screens.

The Board stated that although biometric data is not listed among the special categories of personal data under DPL, GDPR defines "biometric data" as personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Moreover, the Board also referred to GDPR's Recital and a decision rendered by the Turkish Council of State defining and setting out certain criteria regarding biometric personal data and indicated that the data controllers in question are processing special categories of personal data by using biometric information for member identifications.

Referring to other Council of State and European Court of Human Rights decisions and Article 29 Working Party's opinion on developments in biometric technologies as well as the principles set forth under the DPL for legal processing of personal data such as proportionality, the Board concluded that data controllers' practice of requiring their members to use hand and finger print scanning method as the obligatory and only way of obtaining the services provided in the relevant fitness centers is not proportionate.

On the issue of whether explicit consent has been obtained by the data controllers, the Board (i) emphasized that members are required to give their explicit consents for the palm print method under the online membership agreement for the fitness centers, (ii) stated that it appears as though the members would not be able to receive the services provided by the data controllers unless they give their explicit consent and therefore, explicit consent is being presented as a precondition for the provision of services by the data controllers and (iii) thus, concluded that it is not possible to say that explicit consents are given with free will, in the case at hand.

In light of the foregoing, the Board decided to impose an administrative sanction on data controllers for (i) non-compliance with the principle that personal data must be relevant, limited and not excessive in relation to the purposes for which they are processed (Article 4(2) of DPL) since there are alternative methods of member identification and entrance controls, (ii) failing to take all technical and administrative measures in order to ensure an adequate level of security to prevent unlawful processing of personal data considering that the explicit consents have not been duly obtained by the data controllers and (iii) failing to abide by the principle decision rendered by the Board regarding counters, cash desks and tables (2017/62) since data controllers did not take the technical and administrative measures in order to prevent third parties from seeing members' personal information.

The Board also ordered the data controllers (i) to adopt alternative methods for entrance checks and immediately cease processing of biometric information and (ii) to immediately remove hand, finger and palm print information previously obtained and being stored in accordance with DPL and relevant secondary legislation and inform the third parties to whom the relevant personal data has been transferred, if any, regarding the removal activities undertaken by the data controllers.

IV. Sending a Message Containing Irrelevant Content to the Data Subject's Phone Number (Board's Decision 2019/166)

Board's decision of May 31, 2019 with number 2019/166 is rendered upon a complaint claiming that a lawyer sent a text message to his/her phone number with contents relating to a another person (who also happens to be the complainant's nephew/niece).

The complainant indicated that he applied to the data controller regarding the incident and the data controller explained that the incident took place as a result of an employee error, as the employee mistyped one digit in the relevant phone number and consequently, the text message has been sent to the wrong person. However, the complainant argued that the incident could not have resulted as described by the data controller, as his/her number and the nephew/niece's phone number do not only differ by only one digit.

The Board stated that, in the case at hand, the following two data processing activities resulted from one act: (i) name, surname and service number of the third person (niece/nephew of the complainant) being sent to the complainant and (ii) a text message being sent to the complainant and therefore, complainant's personal data being processed without any of the legal reasons listed under DPL.

In light of the foregoing, the Board imposed an administrative fine of TL 50,000 on the data controller for failing to fulfill its obligation to prevent illegal processing of personal data.

V. Sending Multiple Messages on the Same Matter to Data Subject's Phone Number (Board's Decision 2019/159)

Board's decision of May 31, 2019 with number 2019/159 concerns an asset management company which sent a text message on the data subject's phone number on multiple occasions regarding the same matter without obtaining the data subject's explicit consent.

The data subject stated that (i) the text messages did not include an opt-out option, (ii) he/she does not know from where, whom and how his/her personal data has been obtained by the data controller and (iii) he/she applied to the data controller but did not receive a response in the legal time period.

On the matter of failing to respond to the data subject's application, the Board decided not to take action regarding the data controller as the data controller proved through post records that the response has been sent and received by the data subjects in the legal period and also that the response covered all of the areas addressed by the data subject.

The Board also decided not to take action in terms of the contents of the text messages by explaining that the messages has been sent in compliance with banking legislation and rules on financial agreements after the data subject's debt to a bank has been duly transferred to the data controller to ensure that the data subject pays his/her debt to the correct addressee along with explanations regarding payment of the debt. Therefore, the Board concluded that the data processing activity in this case may be carried out without obtaining the explicit consent of the data subject.

On the other hand, the Board stated that the data controller misused its right to send messages by sending the messages with the same contents on different dates and imposed an administrative sanction of TL 20,000 on the data controller for failing (i) to process personal data processed lawfully and fairly and (ii) to take all technical and administrative measures in order to ensure an adequate level of security to prevent unlawful processing of personal data.

Article contact: Gönenç Gürkaynak, Esq. Email: gonenc.gurkaynak@elig.com

(*First published by Mondaq on July 19, 2019*)