GURULKAN ÇAKIR

Turkish Data Protection Authority Continues to Set Precedents on Data Breach

Introduction

Turkish Personal Data Protection Board ("Board") published five decision summaries on its website on July 17, 2019. The decisions set forth the Board's ground rules concerning personal data breaches.

The Board has imposed different amounts of administrative fines to data controllers by taking into account multiple factors. In this article, brief information will be given about these decisions to shed a light on how Turkish Data Protection Authority shape the data protection practice.

Processing of Biometric Personal Data

The Board has given two decisions (No. 2019/81 and No. 2019/165) on processing of biometric personal data for entrances and exits of gym centers. Data subjects claim that there are doubts about processing and safe storage of their certain biometric data including finger prints as well as practices such as public display of their photographs on TV screens.

Although biometric data is not explicitly defined in the Law on the Protection of Personal Data (Law No. 6698) ("the Law"), it is defined under special categories of personal data in General Data Protection Regulation (GDPR) as "*personal data resulting from specific technical processing relating to the physical, physiological*

or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopy data."

The Board sets out certain measures of processing sensitive categories of personal data based on Recitals of the GDPR and decisions of the Turkish Council of State.

Accordingly, data controllers willing to use biometric data for member identifications shall comply with following measures:

- Data processing to authenticate the members by biometric scanning technologies such as the finger print or face must be in accordance with the principles of lawfulness, good faith, accuracy and proportionality.
- Biometric data shall be processed only for specific, clear and legitimate purposes and used only for those purposes.
- The processing shall be relevant and not be excessive in relation to the purposes of the processing.
- Since biometric data shall be protected within the principle of privacy of private life, it should not be kept more than necessary.
- Members are required to give their explicit consents for the storage of their fingerprints, tissue sample and DNA profiles. Otherwise, it would be disproportionate, unnecessary and excessive interference to the right to the privacy in democratic society. (*European Court of Human Rights, S. and Marper v. The United Kingdom (Application number 30562/04 and 30566/04)*)
- Explicit consent regarding biometric data means any informed, specific, freely given and unambiguous indication of the data subject.
- Explicit consent should not be presented as a precondition for the provision of services by the data controllers. The members can benefit from the services provided by the data controllers without their explicit consent.

In light of these contemplated measures, the Board has decided that the processing biometric data by the gym centers is not

proportionate since there are alternative methods for member identification. Besides, explicit consents were not given with free will, because the data controllers requested explicit consent as a precondition to benefit from the gym service.

The decision sheds light on the Board's practice and set forth its ground rules for processing biometric data cases concerning personal data breaches. In this regard, Data controllers such as hospitals or employers who wish to process biometric data shall:

- adopt alternative methods for registration checks,
- obtain explicit consents of data subjects without presenting it as a precondition for the provision of services or recruitment,
- take the necessary technical and administrative measures to prevent third parties from accessing personal data.

Sending Commercial Text Messages without Explicit Consent

The Board's another decision (No. 2019/162) is on the usage of mobile phone number for commercial electronic communication without data subject's explicit consent.

The data subject requested information from the company about the usage of his phone number after receiving a commercial text message from the company. As a data controller, the company is under obligation to respond the requests made by data subjects within 30 days at the latest and free of charge. However, no response was received by the data subject within the prescribed period.

The data subject filed a complaint before the Board for the data controller's failure to respond. The Board evaluated the application and investigated the following issues:

- whether data subjects have the consent to receive commercial texts or notices,
- whether the personal data is processed, and if so, processed for what purposes,
- to whom personal data in Turkey has been transmitted,

- whether personal data has been transferred abroad and by whom it has been transferred, and
- whether data controller is aware of commercial text messages sent to the data subject.

The Board stated that using the data subject's mobile phone number for commercial purposes is regarded as personal data processing and personal data processing shall be based on the legal criteria contemplated by the Law.

Since there was no explicit consent of the data subject for usage of his mobile phone number for commercial purposes, the Board charged the company for not taking all necessary technical and administrative measures to provide a sufficient level of security to prevent unlawful processing or access of personal data.

Before this decision, the only way to claim against unauthorized commercial text messages or notifications was filing a complaint before the Turkish Ministry of Finance via Ministry's Commercial Electronic Message Complaint System ("System"). But the requested result could not be achieved due to its heavy complaint load since over 30.000 complaints filed within the first 8 months of the launch of the System.

Besides, the System does not ensure destruction of personal data but guarantees only the prevention to receive commercial messages without consent. The maximum amount of administrative fine given by the Ministry of Finance was TRY 15,000.

In comparison to the System, the Board's decision provides protection of personal data by ordering data controllers to obtain explicit consent on legal ground while processing personal data.

Sending a Text Message Containing Irrelevant Content

Another decision (No. 2019/166) of the Board was about a lawyer's text message to complainant's mobile phone containing personal data of the complainant's nephew.

The complainant applied to the data controller regarding this message that contained irrelevant content. The data controller

claimed that the message was sent by mistyping only one digit in the relevant phone number and, subsequently, the message was sent to the wrong number by mistake.

Nevertheless, the complainant argued that the content of the received text message belongs to his nephew, and his number and the nephew's phone number do not only differ only by one digit.

The Board stated that sending a text message which contains third person's (the complainant's nephew) name, surname and the service number to the complainant without relying on any of the conditions enacted by the Law violates the obligation to ensure data security.

The Board concluded that data controller must take all necessary technical and administrative measures to ensure the appropriate level of security to prevent unlawful processing of personal data, unlawful access to personal data and to safeguard personal data. The concerning provisions on the liability of data controllers is open to broad interpretation.

The scope of the data controller's liability on data security might include:

- preventing illegal processing of personal data,
- preventing unauthorized access to data, and
- ensuring safe retention of data.

As a preventive approach, to ensure the lawfulness of the processing, data controllers must be careful and adopt internal policies relating to the internal operations of their companies such as drafting privacy policies and making the data available only to authorized personnel.

Consequently, the Board imposed an administrative fine in the amount of TRY 50.000 for failing to ensure data security.

Using Foreign-Based Services for Corporate Email Addresses

The Board (Decision No. 2019/157) ruled that the usage of G-mail servers including storage services (such as Google Drive) which is a foreign-based service, shall be deemed as international data

transfer since the data sent or received through the relevant service is stored in the servers located in foreign countries. Therefore, companies using foreign based services are considered to be transferring the personal data abroad regardless of their intention.

The Board also stated that data controllers who are willing to use the foreign based e-mail and storage services shall comply with the rules on transfer of personal data abroad under the Law.

GURULKAN ÇAKIR

GURULKAN ÇAKIR AVUKATLIK ORTAKLIĞI

Polat İş Merkezi, Offices 28-29
Mecidiyeköy 34387
Istanbul, TURKEY

T +90 212 215 30 00
M info@gurulkan.com
W www.gurulkan.com