Turkish Data Protection Board's Expectations on Compliance: Recent Decisions

Authors: Gönenç Gürkaynak Esq., Ceren Yıldız, Noyan Utkan and Talha Şen, ELIG Gürkaynak Attorneys-at-Law

The Turkish Data Protection Board ("Board") has recently published summaries of several important decisions on certain matters, which may constitute precedents for future cases. All of the decisions below are published on the Data Protection Authority's website on February 12, 2021.

The Board's Decision of December 8, 2020 regarding Right to be Forgotten[1]

The Board conducted an investigation upon a complaint wherein the complainant stated that there had been an academic staff job opening at the public university they are working at, to which their relatives applied and were successful, however social media published false news about the recruitment process, the university conducted an investigation upon the allegations and concluded that there were no irregularities. The complainant claimed that they requested removal of the relevant news from the relevant search engine, and search engine decided not to take any action and that the news articles were affecting their lives and profession, requesting the relevant contents to be de-indexed.

The Board decided through the evaluation it made that, (i) the information provided by the complainant regarding the foregoing incidents were accurate and that the complainant is still working at the same public university, (ii) the contents did not include special categories of personal data, (iii) the incidents dated back to 2020 therefore are considered current, (iv) the contents did not cause any risk for the complainant and could be considered within the scope of journalism activities, (v) contents could cause prejudice against the complainant, but that this is not provable, (vi) there is no legal obligation in publishing of the contents, (vii) the complainant did not publish the contents, (viii) the contents do not relate to a criminal offence. In light of the foregoing, the Board concluded that the search engine's decision of not removing the contents was in accordance with the relevant criteria published by the Board's

[1] Available at https://kvkk.gov.tr/Icerik/6871/2020-927

decision with number 2020/481 and that there were no processes to be undertaken regarding the issue in terms of Law No. 6698 on Protection of Personal Data ("DPL").

The Board's Decision of September 3, 2020 regarding Making Explicit Consent a Precondition for Providing Services[2]

Regarding a data subject's complaint about the data subject applying to a data controller insurance company to renew the health insurance policy issued on behalf of his family and the insurance company requesting explicit consent to renew, Board decided that, since the health insurance policy includes health data, which is a special category of personal data, the health data included in the policy cannot be processed within the scope of Article 6/3 of the DPL and that it can only be processed with the explicit consent of the data subject. Therefore, insurance company requesting explicit consent is in compliance with the law.

This is an important decision in general. Although the Board has not provided further details, asking for explicit consent for renewal might be considered as making explicit consent a precondition for providing services, which may be the grounds for the complaint. However, this decision may also be interpreted as if health data (or any special categories of data) is mandatory to provide the relevant service, explicit consent may be requested as a precondition.

The Board's Decision of June 30, 2020 regarding the Personal Data of the Lawyers Published on Websites[3]

This decision is related to notifications made to the Board from lawyers, of which, their full name, registered bar associations, registry numbers, e-mail addresses and photographs are published on various websites without their consents.

The Board has detected only one website regarding only one of the complainants. The profile in the website only included the e-mail address of that complainant. Board decided that the e-

[2] Available at https://kvkk.gov.tr/Icerik/6878/2020-667
[3] Available at https://kvkk.gov.tr/Icerik/6877/2020-508

mail address is also accessible from Turkish Bar Association's (TBA) website and the relevant websites could have pulled the information from official TBA website and there is no indication that the websites broadcast such information for a purpose other than the purpose for publication of that information in TBA website and the data subjects are granted the means to delete or rectify the personal data. Therefore, this matter is not against the processing conditions under Article 5 and general principles under Article 4 of the DPL since the personal data were made public by the data subject to be published on TBA website.

This is also an important decision since third party websites using the public information for the same purpose is considered in compliance with the DPL even data subject has not consented.

The Board's Decision of January 30, 2020 regarding the Determination of the Data Controller and Data Processor[4]

The Board published a decision summary regarding the matters that should be taken into account in the determination of the data controller and data processor and which will be fulfilling the obligation to inform. The Board decided that the obligation to inform which is regulated in Article 10 of the Law No. 6698 can also be performed by the data controller itself or by a person authorized by the data controller as well as the data processor. In this decision, the Board also underlines the criteria of data controller and processor.

Those who fulfill most of the following criteria are considered as data controllers:

- Collection and collection method of personal data,
- The types of personal data to be collected,
- Which individuals' personal data will be collected,
- Deciding on the processing of personal data and who will process it,
- Deciding on the basic elements of the processing (which personal data will be collected, for what purposes the collected data will be used and how it will be processed, how long the data

[4] Available at https://kvkk.gov.tr/Icerik/6874/2020-71

will be retained, what the data retention policy will be, who will be authorized to access the data, who will be the recipients, etc. can be shown as examples)
- Whether the collected data will be shared, and if so, with whom,
- Being able to make decisions at a high level in the processing of personal data without taking any orders or instructions,
- Dealing directly with the data subjects,
- Appointment of a data processor to carry out data processing on their behalf,
- Taking advantage of the processing activity.

Data controller may appoint a data processor who is authorized with the following through a data processing agreement:

-Which IT systems or other methods will be used for collection of personal data
-Through which method the personal data will be retained
-Details of the security measures that can be taken for protection of personal data
-Using which method the data will be transferred
-Method for correctly operating personal data retention periods
-Methods for deletion, destruction or anonymization of personal data.

Those who fulfill most of the following criteria are considered as data processors:

-Taking instructions from another
-Not having the authority to make decisions in collection of personal data from persons
-Not having the authority to decide on how the data can be exposed, who can access such data
-Not having the authority to decide on data retention process
-Not having responsibility for the consequences of data processing
-Whether there are any decision-making mechanisms regarding data processing within the scope of authorities granted by the data controller under legally binding agreements such as with a data controller.

The Board's Decision of January 30, 2020 regarding Processing Personal Data without Relying on Any Processing Conditions[5]

The Board conducted an investigation upon the complaint of a person who claimed they received multiple informative messages regarding several electricity service membership numbers regarding various issues and who requested his/her contact information to be deleted from the records related to the relevant membership agreements. The company has not provided to response and kept sending the messages. The company claimed in its defense that, contact information of the relevant data subject was updated but no documents were sent to the Board confirm it. The Board indicated that the request should be considered a request of "correction" of personal data instead of deletion. The Board found that the data controller made it difficult for data subject to exercise its rights. Consequently, the Board instructed the data controller to respond timely and completely to such requests, while also imposing a monetary fine of TL 100,000 (approximately EUR 11,760) on the data controller on the grounds that the data controller did not take the necessary administrative and technical measures.

This decision is important as it demonstrates that the Board is not bound with the legal basis of the complaint and can even change the nature of it during investigation.

The Board's Decision of December 1, 2020 regarding Biometric Data[6]

Upon a civil servant's complaint, Board conducted an investigation regarding a governmental institution's implementation of fingerprint method for supervising employee shifts. The Board found the relevant methods used by the institution to be in violation of the DPL on the grounds that biometric scanning should only be used when extreme security measures are needed and since as a result of COVID-19, the current method of supervision of employees are made through wet signature, it is understood that at the moment, extreme security measures are not necessary for the institution, and that the institution is able to supervise its employees through alternative methods without processing its employees' biometric data.

[5] Available at https://kvkk.gov.tr/Icerik/6873/2020-66
[6] Available at https://kvkk.gov.tr/Icerik/6872/2020-915

Therefore the Board found that taking fingerprints of employees for the purposes of surveilling employee shifts violates the proportionality principle governed under paragraph (ç) of Article 4 of the Law No. 6698.

Although it is related to a public institution and a civil servant's complaint, it is important in general as biometric scanning for surveilling shifts is a commonly used practice. The data controller claimed that the fingerprints cannot be extracted as the fingerprint data is encrypted, becomes a template and then matched with the relevant person. This methodology is often used in fingerprint scanning systems. However, the Board has not found this defense applicable and emphasized that explicit consent was needed for processing. The Board also emphasized, in line with its previous decisions, that if extreme security measures are not needed and alternative methods are applicable, biometric data should not be taken.

The Board's Decision of January 27, 2020 regarding Unauthorized Access to E-Mail Account[7]

The Board investigated the matter upon the complaint of the data subject claiming that his/her corporate e-mail account was accessed without permission and against the law, his/her access settings were changed and he/she requested deletion of all data in his/her e-mail account from the data controller. Data controller indicated in its defense that the data subject was a manager in the company subject to an investigation for misuse of duty for transferring money from corporate accounts to various bank accounts, the data was obtained from the backups, which were created upon the data subject's own request, the e-mail messages were taken to investigate the issue, which is subject to a commercial lawsuit and data subject's criminal complaint was rejected.

The Board decided that the processing is in compliance with the law since processing was *"necessary for compliance with a legal obligation to which the data controller is subject"*.

[7] Available at https://kvkk.gov.tr/Icerik/6869/2020-59

This is an important decision as it is an example for application of the relevant processing condition.

The Board's Decision of September 17, 2020 on Sending Lien Notification to the Relatives of a Debtor[8]

According to the decision, the execution office investigated the name and addresses of the debtors' relatives and sent lien notifications to them. The data controller indicated in its defense that the lien notification was sent in accordance with the Article 89/1 of the Law No. 2004 Enforcement and Bankruptcy Law ("Law No. 2004") which authorizes execution office to send notices to any third party who possibly holds debtor's receivables, therefore, the said process was in accordance with the law. Following the data controller's response, the Board investigated the matter and concluded that the notices sent by the execution office, were in accordance with the Article 89/1 of the Law No. 2004. Therefore Board decided that this personal data processing activity is lawful due the fact that this activity is based on the processing condition of "*it is expressly provided for by the laws*".

The Board's Decision of October 30, 2019 regarding Destruction of Special Categories of Personal Data[9]

The Board received a complaint from a doctor regarding the collection and recording of blood, serum and tissue samples for scientific research projects by a hospital and deterioration of said samples as a result of negligence and error of the said hospital which constitutes a violation of obligations regarding data security in accordance with the Article 12 of the Law No. 6698. The Board requested defense from the data controller on the matter and data controller indicated in its defense that deterioration of said samples caused by a fault which kept under records and said samples are not usable for scientific purposes. Within the information shared by the data controller and complainant, Board stated that, collection of blood, serum and tissue samples with barcodes make it possible to match these samples with the patients which constitutes a personal data processing activity. However Board further stated that, this processing activity falls outside of the scope of the Law No. 6698 as this

[8] Available at https://www.kvkk.gov.tr/Icerik/6879/2020-710
[9] Available at https://www.kvkk.gov.tr/Icerik/6876/2019-316

processing activity is pursued on a scientific purpose which is regulated under the Article 28 of the Law No. 6698 as one of the exceptions.

The Board's Decision of February 6, 2020 regarding the Rectification and Erasure of Personal Health Data[10]

The decision states that the DPA received several complaints from data subjects stating that their recorded health data (especially psychiatric health records) constitutes problem in their daily life and requesting rectification and erasure of these personal health data from the records. Board started an investigation and requested the data controller Ministry's defense on the matter. Data controller indicated in its defense that the said personal data was processed as per the Article 6/3 of the DPL, which does not require the data subjects explicit consent, the legal condition on which the data processing activity is based has not yet disappeared and the erasure of the health records in question may constitute a threat to public health and safety. Data controller also indicated that for diagnoses that are not proven to be inadvertently recorded; data subject should apply to provincial health directorate.

The Board evaluated the matter and stated that; regarding the rectification of the personal health data, Article 13 of the Regulation on Personal Health Data should govern, which directs the relevant persons to provincial health directorates for inadvertent records, legal condition which the data processing activity is based on is still valid and the personal data is processed as per Article 6 of the DPL, therefore decided that no action should be taken regarding the request for erasure.

The Board's Decision of January 27, 2020 regarding the Personal Data which is Processed within the Scope of White Code Procedure[11]

The Board conducted an investigation upon a complaint wherein the complainant stated that his/her personal data which was accessed from hospital records was processed following an argument between hospital personnel and the complainant, after the complainant left the hospital. The complainant applied data controller hospital and data controller stated in its response that they followed the procedure on the 2016/3 Circular of the Legal Counsel of the

[10] Available at: https://kvkk.gov.tr/Icerik/6875/2020-93
[11] Available at: https://www.kvkk.gov.tr/Icerik/6870/2020-63

Ministry of Health on Legal Aid and White Code Procedure ("Circular No. 2016/3") and said personal data only shared by the persons/entities that are under confidentiality.

The Board evaluated the defense of the data controller, and stated that, the processing activity in question was in accordance with the Circular No. 2016/3 which falls under the scope of Article 5/2/ç of the DPL (*It is necessary for compliance with a legal obligation to which the data controller is subject*). Consequently, Board decided that the processing activity in question was in accordance with the DPL.

The Board's Decision of December 26, 2019 regarding the Necessity of Signing Confidentiality Agreement with Public Officer[12]

According the decision; duties, rights, obligations and responsibilities of the public officers are governed under Law No. 657. Pursing to Law No. 657, the public officers are obliged to comply with the principles specified in the law and other legislation, to carry out their duties with care and attention. Also it is regulated that in the event that individuals are harmed as a result of the fault of a public officer, the relevant person must apply directly to the relevant institution instead of the public officer. Recourse relationship between the public institution and the public officer is regulated in the Law No. 657 and its relevant regulations. In this context, it would not be correct to sign a confidentiality agreement between the public institution and its personnel due to the reason that such agreement will affect the current recourse relationship between the public institution and its personnel.

Board consequently stated that, the issue of signing an employee confidentiality agreement, which is mentioned in both the Personal Data Security Guide and the Board decision numbered 2018/10, is applicable to the employees subject to employment agreement under the orders and instructions of an employer, and to employees working in public institutions and organizations who are not subject to Law No. 657.

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

(First published by Mondaq on February 22, 2021)

[12] Available at: https://www.kvkk.gov.tr/Icerik/6868/2019-393