Data Breach: Evaluation of the Recent Precedents of the Turkish Data Protection Board

Authors: Gönenç Gürkaynak Esq., Ceren Yıldız, Derya Başaran, ELIG Gürkaynak Attorneys-at-Law

Over the last four months, the Turkish Data Protection Board ("Board") concluded many data breach investigations and has recently published several decisions on its own website. In light of these recent decisions, it is seen that the Board made its evaluations and imposed certain administrative fines mainly based on two topics: (i) whether the necessary technical and administrative measures have been taken to ensure data security, and (ii) whether the obligation to notify the Data Protection Authority ("DPA") and the data subjects affected by the data breach "as soon as possible" has been fulfilled. Below is a snapshot of the criteria taken into consideration by the Board in its assessments of data breach, in light of the decisions taken over the past four months.

Necessary Technical and Administrative Measures to Ensure Data Security

While the Board evaluates whether the administrative and technical measures were already in place, it also considers the number of the data subjects affected by the data breach, the severity of risks imposed on data subjects, the nature of the personal data affected by the breach, and the size of the data controller. Needless to say, the Board conducts its evaluations within the scope of the Personal Data Security Guide (Technical and Administrative Measures)[1]. The Board also evaluates whether the personal data security monitoring is carried out at appropriate time intervals, whether the necessary tests are carried out by looking at the time interval in which the data breach occurred, and considers the training provided by the data controllers for their employees.

In one of the recent decisions of the Board, the Board evaluated a systemic error that caused the data breach as an exceptional case and apparently imposed a reduced administrative fine on the data controller who did not take the necessary technical and administrative measures to ensure data security[2]. In an event where the data breach was identified 13 minutes after its occurrence and has been terminated 2 hours after its occurrence, the Board decided not to take any action against the data controller at that stage considering the low possibility of the breach to have a negative effect on the relevant data subjects[3]. It is seen in 3 other decisions that the Board decides to take no action wherein

[1] Available at https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf
[2] Available at https://www.kvkk.gov.tr/Icerik/7032/2020-532
[3] Available at https://www.kvkk.gov.tr/Icerik/7020/2020-957

the data breach affects the personal data of one person[4] and, the possibility of the data breach having a negative effect on the relevant data subjects is low[5].

Notification Obligation

The Board considers whether notifications have been made to the DPA and the relevant data subjects affected by the data breach within the 72-hour period starting from the moment the data breach was learnt by the controller, based on its 2019 decision with number 2019/10[6], and generally imposes administrative fines for the notifications that have been made after 72 hours. As an exception to this situation, the Board, in one of its decisions about a multi-national data controller, took into account the multi-national status of the data controller and the time required for the determination of the countries where the affected data subjects are located and the notification requirements of the relevant countries and evaluation of such and ruled that a one-month period for notifying the DPA was reasonable[7]. In another decision wherein the data controller residing abroad was 8 days late for notifying the DPA, and the Board, by considering that the data controller has carried out an investigation to determine whether the relevant data subjects in Turkey were also affected by the data breach, decided that the 8-day period was reasonable for notifying the DPA[8].

The Board also made an exception for the pandemic in one of its recent decisions, wherein the Board decided that there is no action to be taken against the data controller who exceeded the 72-hour notification period by 1 full day, considering that a 1-day delay was reasonable due to the pandemic[9]. However, in another decision, even though the Board evaluated that the data controller had taken the necessary technical and administrative measures, it instructed the data controller to be more careful about notifying within 72-hour period.

In another decision wherein the Board imposed an administrative fine on the data controller who did not take the necessary technical and administrative measures to ensure data security, although the data breach was not reported to 95 persons out of 172 affected data subjects and the remaining 77 persons were notified a month after the identification of the data breach, the Board decided to remind the data controller on notifications and did not impose administrative fines in this regard[10].

[4] Available at https://www.kvkk.gov.tr/Icerik/7019/2020-935
[5] Available at https://www.kvkk.gov.tr/Icerik/7018/2020-816
[6] Available at https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi
[7] Available at https://www.kvkk.gov.tr/Icerik/7035/2020-934
[8] Available at https://www.kvkk.gov.tr/Icerik/7026/2020-50
[9] Available at https://www.kvkk.gov.tr/Icerik/7016/-2020-567
[10] Available at https://www.kvkk.gov.tr/Icerik/6995/2020-466

Addition to the foregoing, it is worth noting that the Board is evaluating whether the minimum elements specified in its September 12, 2019 dated decision with number 2019/271 are included in the data breach notifications provided by the data controllers to the affected data subjects[11].

Administrative Fines

As the minimum amount for the administrative fine for failure of providing administrative and technical security measures is minimum 29,500 Turkish Liras and maximum 1,966,860 Turkish Liras for 2021, we see that the highest amount of the administrative fines imposed by the Board in the last 4 months is 600,000 Turkish Liras[12], and the average of the fines imposed is 187,000 Turkish Liras. Below is a breakdown of the administrative fines over the past 4 months, imposed due to the failure of taking the necessary technical and administrative security measures:

(i) The average of the fine amount of latest decisions imposed by the Board due to lack of providing technical security measures: 186,800 Turkish Liras

(ii) Number of decisions that imposed fines less than 100,000 Turkish Liras: 6

(iii) Number of decisions that imposed fines between 100,000 – 200,000 Turkish Liras: 4

(iv) Number of decisions that imposed fines between 200,000 – 400,000 Turkish Liras: 2

(v) Number of decisions that imposed fines between 400,000 – 600,000 Turkish Liras: 2

(vi) The highest fine imposed in the last four months is one decision for 600,000 Turkish Liras.

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

(First published by Mondaq on September 9, 2021)

[11] Available at https://kvkk.gov.tr/Icerik/5547/2019-271
[12] Available at https://www.kvkk.gov.tr/Icerik/6993/2021-407