Data Breach Notification Obligation In Light of Turkish Data Protection Authority's Recent Decisions

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

I. Data breach under Turkish laws

There is no specific definition of "data breach" under the Turkish data protection law ("Turkish DP Law"). However in terms of notification obligations, "illegal seizure of or access to personal data" is considered as a data breach. Under the Turkish DP Law in case of a data breach (illegal seizure of or access to personal data), the data controller is obliged to notify the breach to (i) the data subjects (affected individuals) and (ii) the Turkish Personal Data Protection Authority ("Turkish DPA"), within the shortest time ("shortest time" applies to both notifications). There is no distinction as to eligibility of the data breach for notification and there are no exceptions provided under the legislation for the breach notification.

II. Scope of data breach notification obligation

Data breach notification requirement of data controllers is principally regulated under Article 12/5 of Turkish DP Law. Article 12/5 of Turkish DP Law provides that *"in case of a data breach, data controller is obliged to notify the breach to the data subjects and the Turkish Personal Data Protection Board, within the shortest time*". Although the term "the shortest time" is not specified, Turkish DPA interprets and applies "the shortest time" for notifying Turkish DPA as "within 72 hours after becoming aware of the breach" (Turkish DPA's decision no. 2019/10), also in line with the GDPR, which requires notification without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. In the event that the data controller is unable to notify the Turkish DPA within 72 hours for a justified reason, the data controller's notification should also include the reasons of the delay as well. The information on the data breach, its effects and the measures that are taken should be recorded and kept ready for Turkish DPA's inspection.

Furthermore, data controllers should have a data breach response plan in place, defining the issues such as whom the data breach will be internally reported to and who will be responsible for the legal notifications and evaluation of the possible effects of the breach, and such plan should be regularly reviewed and revisited.

III. Notification of the breach to the Turkish DPA

"Data Breach Notification Form" issued by the Turkish DPA should be used while notifying the Turkish DPA. If all of the information requested in this form cannot be provided at the

same time, data controller is obliged to provide the outstanding information later without causing undue delay. Notification should either be sent by e-mail to the e-mail address provided by the Turkish DPA for data breach notifications or by post to the Turkish DPA's notification address with all supporting documents attached to the form. Turkish DPA requires that data controllers to submit notifications hard-copy through post or by hand. The notification needs to be submitted in Turkish language, signed by an authorized signatory and should include the company seal.

IV. Notification of the breach to the data subjects

In terms of notifying the data subjects, data controller should notify data subjects within the reasonably shortest time, same as notifying the Turkish DPA. As per the Turkish DPA's decision no. 2019/271, such notification should be made directly to the data subject, if the contact address of the data subject is known. If the data subject's contact address is not known to the data controller, then data controller must notify the data subject through other proper communication methods such as publishing a notification on its website.

According to the same decision, the language of the data breach notification to the data subjects should be plain and the data breach notification should include the following elements:

(i) The time of the data breach,
(ii) Information on the personal data affected from the data breach based on personal data categories (by distinguishing personal data and special categories of personal data),
(iii) Possible consequences of the data breach,
(iv) Measures taken or proposed to reduce the negative effects of data breach,
(v) The name and contact details of the contact persons who will provide information to the data subjects regarding the data breach or the specific address of the data controller's website, call center and any other communication methods.

V. Consequences of non-compliance in light of the recent penalties imposed by the Turkish DPA

Failure to comply with the data breach notification obligation is subject to an administrative fine ranging from TL 15,000 up to TL 1,000,000 (subject to updates per the yearly reevaluation rates). Turkish DPA strictly and seriously enforces the obligation to notify the authority and data subjects on data breaches and issued remarkable amounts of penalties against a variety of data controllers in this regard.

In a recent decision issued on September 18, 2019 with the number 2019/169, the Turkish DPA unanimously decided to impose an administrative fine in the amount of TL 450,000 on Facebook due to failure to notify a data breach to the Turkish DPA.[1]

Similarly the Turkish DPA granted another decision on August 28, 2019 with the number 2019/254 and imposed an administrative fine on "S Sans Oyunlari A.S" in the amount of TL 30,000 for failure to notify data subjects of a data breach.[2]

In another decision issued on August 28, 2019 with the number 2019/255, the Turkish DPA decided to impose an administrative fine on a tourism company in the amount of TL 100,000, due to their failure to (i) notify the data subjects and (ii) notify the Turkish DPA within "shortest time" as required under the law.[3]

The foregoing are only some examples of the Turkish DPA's enforcement of the data breach notification obligation which are publicly available. Turkish DPA strictly applies this requirement and requires data controllers to notify an incident to the Turkish DPA even if the specifics of the incident are not yet certain (e.g. even if the data controller has not yet determined whether data subjects in Turkey are certainly affected). Data controllers will need to establish data breach response plans or protocols, determine and allocate duties for handle data security incidents and data breaches to make sure they duly comply with their notification obligation vis-à-vis the Turkish DPA and the data subjects in Turkey and avoid possible administrative fines.

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

(*First published by Mondaq on November 7, 2019*)

[1] Turkish DPA's decision with the number 2019/169 available at https://kvkk.gov.tr/Icerik/5534/2019-269
[2] Turkish DPA's decision with the number 2019/254 available at https://kvkk.gov.tr/Icerik/5535/2019-254
[3] Turkish DPA's decision with the number 2019/255 available at https://kvkk.gov.tr/Icerik/5537/2019-255