Client Alert | Data, Privacy & Cybersecurity

New Standardization for Data Breach Incidents in the Scope of Turkish Personal Data Protection Legislation

February 2019

Authors: **Emre Özşar**, **Selin Kaledelen**, **Zeynep Ülkü Kahveci**

Article 12 of the Law no. 6698 on the Protection of Personal Data ("**PDPL**") regulates security of personal data. In addition to PDPL, the Turkish Personal Data Protection Board (the "**Board**") published a guideline on this matter (i.e. Guideline on Security of Personal Data-Technical and Administrative Measures).

Taking into account the data breach notifications published on the Board's website, there was a controversy in relation to the timing of the data controller's notification to the Board for data breaches. The Board's recent decision provided clarity on the subject and this decision is also in line with the General Data Protection Regulation (GDPR- 2016/679).

Background

Pursuant to Article 12, paragraph (1) of PDPL, a data controller is obliged to take any and all kinds of technical and administrative measures in order to:

- prevent illegal processing of personal data;
- prevent illegal access to personal data; and
- safeguarding personal data;

and pursuant to paragraph (5) thereof, if the processed personal data is accessed by third persons illegally, then the data controller shall notify the relevant breach to the data subjects and to the Board as soon as possible and depending on the nature of the breach if necessary, announce it in his/her website or through other means.

The following decision adopted by the Board dated January 24, 2019, numbered 2019/10, is rendered for the purposes of clarifying the current ambiguities and setting forth the applicable standards.

What is new?

1. As soon as possible i.e. "72 hours rule" for data breach incidents

The expression "as soon as possible" in article 12, paragraph 5 of the PDPL shall be interpreted as 72 hours. This means that the data controller shall notify this situation to the Board as soon as possible but in any case within 72 hours.

Moreover, once the data subjects who are effected from such data breach are determined, then the data controller shall serve a notice (in relation to the respective breach) to such data subjects within a reasonable period of time. The data controller is obliged to reach the data subjects directly if their contact details are available, or otherwise, through by other means (e.g. such as making an announcement via its website).

If the data controller fails to serve such notification within 72 hours without any solid grounds, then reasons for such delay needs to be separately notified to the Board via serving an additional notice.

Please note that a data controller's failure to fulfil its obligation to (i) ensure data security, and (ii) comply with this Board decision mandating the 72-hour notification rule will result in an administrative fine in an amount up to TL 1,000,000 for each obligation. Along with the data controller, data processors will have joint liability over the security of data it is processing. Even though the 72-hour obligation for the notification only applies to the data controller, data processors will be jointly liable with data controllers for any incompliance with this obligation.

2. Personal Data Breach Notification Form

The following "Personal Data Breach Notification Form" ("**Form**") shall be used and attached with? the notice to be served to the Board. If, for any reason, it is not possible to provide the information included in the Form immediately after the data breach, such information shall be provided separately without any delay.

The form consists of five parts, namely "*Information About the Data Controller*", "*Information About the Data Breach*", "*Possible Consequences*", "*Consequences of the Cyberattack, If Any*" and "*Precautions*". Below is a brief summary of the information requested under the Form:

- Information about the data controller;
- Details on the data breach: date, source, and time of detection of such breach (e.g. storage of data in insecure platforms, malware, accident etc.);
- Category of data affected by the data breach: personal data/ sensitive data;
- Estimated number of people affected by the data breach;
- Groups of people affected by the data breach (e.g. employees, members, students, children);
- Possible consequences foreseen by the data controller;
- Estimates in relation to recovery (whether the duration of recovery period is foreseeable);
- Consequences of the cyberattack, if there is any (whether the information system of the data controller is affected, the effects on the system);
- Precautions (whether affected employees received any training on data privacy in the last one year, administrative and technical precautions taken before the data breach took place, whether other data protection authorities located abroad or related institutions have been informed).

3. Risk analysis

Three different categorizations in relation to risk analysis are provided on the Form.

a. Negative Impacts of the Data Breach on Data Subjects

An explanation in relation to the "possibility of material negative impacts suffered by data subjects as a result of the data breach" is included at the end of the Form. Accordingly, notifying data controllers should also assess the potential impact of the data breach on data subjects. The nature of the data breach, cause of the data breach, type of data affected by the data breach, precautions taken to mitigate the impacts of the data breach should be taken into account for such assessment.

Risk assessment may indicate *low level of risk* (data breach does not cause any negative impact on data subjects or such impact is negligible), *medium level of risk* (data breach may cause negative impact on data subjects but such impact is not major) or *high level of risk* (data breach causes a serious level of negative impact on data subjects).

b. Impacts of the Data Breach on the Institution

The Form contains a chart on the risk analysis of the data breach as located below.

Impact of the Data Breach	**Explanation**
High	You have lost your ability to provide all kinds of significant services to all of your users.
Medium	You have lost your ability to provide all kinds of significant services to some of your users.
Low	There is no loss of activity or there is very low level of loss of activity and you can provide all kinds of major services to all of your users.
Unknown	

c. Impacts of the Cyberattack (if any) on the Institution

In case the data breach is a result of a cyberattack, the data controller should also provide details in relation to the details/impacts of the cyberattack on the institution.

Impact of the Cyberattack	**Explanation**
High	You have lost your ability to provide all services provided through information systems to all of your users.
Medium	You have lost your ability to provide all services provided through information systems to some of your users.
Low	There is no loss of activity or there is a negligible level of loss of activity and you can provide all services provided through information systems to all of your users.
Unknown	

Please note that it is not feasible to expect all data controllers to have the required technical knowledge to assess the risks related to a data breach and/or cyberattack. Supplementary technical expertise will be required.

4. Data Breach Intervention Plan

In case of data breach, the data controller is obliged to prepare a data breach intervention plan, regulating the persons to whom reports will be sent, the notices to be served within the scope of the PDPL and the persons who will be liable in terms of evaluating the possible consequences of the data breach and it shall review and update such plan regularly.

GKC Partners
Ferko Signature
Büyükdere Cad. No: 175 Kat: 10
Levent 34394
Turkey

T +90 212 355 1300