Consequences of failure to meet data security obligations

April 04 2017 | Contributed by ELIG, Attorneys-at-Law

AUTHORS

Gönenç Gürkaynak

İlay Yılmaz

Introduction

Under the Data Protection Law, data controllers must take all necessary technical and administrative measures to ensure an adequate level of security to:

- prevent unlawful processing of and access to personal data; and
- safeguard personal data.

A data controller should provide the required supervision within his or her own institution or agency or outsource this service to an independent third party to ensure compliance with the Data Protection Law. Data controllers and parties processing data cannot disclose this data to other parties or use it for any purpose that violates the Data Protection Law. This obligation continues after the persons who engage in the processing of personal data leave office.

Notification of breach

If processed personal data is unlawfully obtained by others, the data controller should notify the data subject and the Data Protection Board as soon as possible. If necessary, the board will publicise such an issue on its website or via other means deemed appropriate. These provisions are not effective in practice and will be clarified once the board is established.

The term 'as soon as possible' does not clarify a precise deadline for a data breach notification. Under the EU Data Protection Directive (95/46/EC), there is no generally applicable obligation regarding notification of data breaches. The EU General Data Protection Regulation states that in the event of a personal data breach, data controllers must notify the relevant data protection authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it". If notification is not made within 72 hours, the controller must provide a "reasoned justification" for the delay.

In this regard, the abovementioned approach might be considered by the board while also interpreting the notification period for data breaches under the Data Protection Law. On receipt of notification, the board may announce the issue on its own website or through other means, as deemed appropriate.

As the period for notifying the board and the data subject of a data breach is uncertain, this obligation should be promptly fulfilled by evaluating the situation on a case-by-case basis. To avoid any delay and ensure compliance with the notification obligation, a data controller can issue an internal data breach protocol explaining how to manage data breaches within the scope of an immediate action plan and prepare template notification texts for both data subjects and the board.

Security obligations

Under the Data Protection Law, data controllers must take all necessary technical and administrative measures to provide an adequate level of safety to prevent the unlawful processing of, access to and protection of personal data. However, the Data Protection Law does not specify the "necessary technical and administrative measures". The International Organisation for Standardisation (ISO) has a set of standards for technical data security measures (ISO/IEC 27000). The relevant standards include guidance for helping organisations to keep their information assets secure. ISO/IEC 27000 includes:

- standards for information security management systems;
- a code of practice for information security management;
- information security management system implementation guidance;
- information security risk management;
- requirements for bodies providing information security management system auditing and certification; and
- guidelines for information security management system auditing (focused on the management system).

The Data Protection Law makes no reference to information security-related standards. They are expected to be set out under secondary legislation, which should come into force on April 7 2017 under the Data Protection Law. Therefore, it is unclear whether the ISO standards will comply with the information security requirement under the Data Protection Law.

Liability

With respect to data safety, the data controller and data processor are jointly liable. The Data Protection Law explicitly states that if personal data is processed by another real or legal person on behalf of the data controller (ie, the data processor), the data controller will be jointly liable with such persons to provide data security.

For example, in case of a data security violation, the data subject may target both the data controller and data processor or only the data controller. These parties may resolve the dispute based on an internal agreement or the data controller may recourse to the data processor under general law.

Section 5 of the Data Protection Law regulates crimes and minor offences. Any data processor who does not comply with the regulation will be punished under the Criminal Code or be subject to an administrative fine ranging from TRY15,000 to TRY1 million, depending on the nature of the offence.

For further information on this topic please contact Gönenç Gürkaynak or İlay Yılmaz at ELIG, Attorneys-at-Law by telephone (+90 212 327 17 24) or email (gonenc.gurkaynak@elig.com or ilay.yilmaz@elig.com). The ELIG, Attorneys-at-Law website can be accessed at www.elig.com.
