YAZICILEGAL
NEWSLETTER
www.yazicilegal.com
A. Levent Mah. Yasemin Sok. No.13 Beşiktaş 34340 İstanbul **T.** +90 212 269 02 27 **F.** +90 212 269 02 28 **E.** info@yazicilegal.com

RECENT DEVELOPMENTS ON THE DATA PROTECTION LEGISLATION

Changes brought by the Personal Data Protection Board (the "Board")

Personal Data Protection Board Decision No. 2018/10 (the "**Decision**") was published by the Board in the Official Gazette dated March 07, 2018 numbered 30261, introducing the adequate measures to be taken in processing the special categories of personal data as stated in Article 22 of Law on Protection of Personal Data (No. 6698) (the "**Law**"). Special categories of personal data indicated in Data Protection Law Article 6 are; biometric and genetic data, race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, appearance and clothing, association or foundation or trade union membership, health, sexual life, criminal conviction and security measures.

The Decision has been taken on January 31, 2018, and has entered into force on the date it was published in the Official Gazette. As the Board has been authorized to determine the adequate measures for the processing of sensitive data under both Articles 22 and 6/4, and the lawful processing has been conditioned to comply with the measures to be determined by the Board; the Decision and the measures thereunder are binding. Correspondingly, the imposition of an administrative fine of 25,000 to 1,000,000 Turkish Lira for the failure to abide by the Board decisions under Article 18 of the Law, may be applied in case of failure to comply with the measures described in the Decision. This may also be subject to imprisonment of 18 months to 54 months under Article 135 of the Turkish Criminal Code to the extent that the action may be regarded as unlawful processing.

The measures to be taken in order to ensure lawful processing of sensitive data are supported by the Personal Data Security Guide (the "**Guide**"). Being advisory in nature, the Guide sets forth details and procedures to assist the compliance process for both sensitive and regular personal data. To note, there are no similarly detailed or binding measures to be used for the lawful processing of regular personal data, yet the application of the measures in the Guide will result in a comprehensive protection structure.

The Decision determines the required actions for the security of sensitive personal data under five sets of measures, as follows:

<u>Separate Policy and Procedure for the Security of Sensitive Personal Data</u>

The lawful processing terms for sensitive and regular personal data differ from each other. Therefore they cannot be evaluated or examined under the same procedure. Data controllers must categorize the data they process and establish and use a stricter protection regime where sensitive data are concerned.

<u>Measures Concerning the Employees who Process Sensitive Data</u>

As employees constitute the agents of processing under a data controller,

- they must be trained periodically on the regulatory framework and the security measures,
- confidentially agreements must be signed with them,
- the scope and the periods of their access authorizations must be explicitly defined,
- access authorizations must be controlled on a periodic basis,
- the access authorizations of the employees who leave work, or whose positions are changed must be revoked immediately, and the inventories assigned to them must be returned.

<u>Measures for the Electronic Processing Environments</u>

- Sensitive data must be stored using cryptographic methods,
- The cryptographic keys must be kept in secure and varying platforms,
- The actions executed on sensitive data must be securely logged, permitting retrospective analysis,
- Security updates for the processing environments must be installed regularly, the required security tests must be executed and the results of the tests must be recorded, as the usage of older versions of software constitute one of the major reasons behind the failure of data protection,
- Where sensitive data is accessed through a software, the access authorizations of the users of such software must be defined, the required security tests must be periodically executed, and the results of the tests must be recorded,
- Remote access to data must be secured with a two-stage identity authentication system.

Measures for the Physical Processing Environments

- Adequate security measures must be taken against force majeure events that may destruct the sensitive data, such as fire, flood, theft, etc.
- The physical environments in which the sensitive data is processed must be secured to prevent unauthorized entry.

Measures for Transfer

- The sensitive data must be encrypted for transfers via e-mail and corporate e-mail address or Registered Electronic Mail Method must be followed,
- Transfers that must be done through the usage of memory sticks, CDs or DVDs, the sensitive data must be encrypted and the cryptographic keys must be stored in separate platforms,
- VPN or the sFTP method must be used where the transfer is between the servers in different physical environments
- Where documents must be transferred in hard copies, the transfer must be in "classified information" format to prevent theft, loss or unauthorized access.

Despite the lack of instances where the Board has previously used its discretion to fine failures to abide by the above-mentioned measures, the Board is expected to look closer into the measures to be taken for the security of sensitive data, as there are certain recent decisions on the unlawful transfer as a whole.

Communiqué on Procedures and Principles regarding the Obligation to Enlighten (the "Communiqué")

The Communiqué was published in the Official Gazette No. 30356 dated March 10, 2018, and entered into force on the date of its publication. The Communiqué has been prepared in order to set forth the principles and procedures on the obligation to enlighten in accordance with Article 10 of Law No. 6698 on Personal Data Protection (the "**Law**") dated May 24, 2016. According to Article 10 of the Law; the relevant persons must be informed during the collection of the personal data by the data controllers or their authorized persons (representatives) and the provided information shall include the following subject matters;

- The identity of the data controller and their representatives,
- For what purpose the personal data will be processed,
- To whom and for what purpose the personal data might be transferred,
- Collection method of the personal data and its legal basis,
- Persons' other rights outlined in Article 11 of the Law.

The physical environment in which the obligation to enlighten shall be made are listed as "physical, or electronic environments such as oral, written, voice recording, call center, etc." and similar arrangements can be used as a communication way. The notable ones of the procedures and principals further introduced by the Communiqué required to be followed by the data controllers are as follows;

- Based on other processing conditions set forth in Law or the relevant persons' informed consent, the obligation to enlighten shall always be fulfilled in any case the personal data is processed.

- When the purpose of processing the personal data changes, the obligation to enlighten shall be otherwise fulfilled for the new purpose before processing the personal data.

- If the personal data are processed with different purposes in each of the units of the data controller, then the obligation to enlighten shall be otherwise fulfilled at each unit.

- The information provided to the relevant persons shall be in compliance with the information submitted to the Data Controllers Registry.

- The obligation to enlighten is not dependent on the relevant persons' request.

- It is the responsibility of the data controller to demonstrate that the obligation to enlighten has been fulfilled.

- If the processing of the personal data is executed based on the explicit consent requirement, the consent and the obligation to enlighten shall be fulfilled separately.

- The purpose of the processing the personal data which shall be explained to the persons within the scope of the obligation to enlighten shall be specific, clear and legitimate. While fulfilling the obligation to enlighten the data controllers shall avoid general and vague statements.

- The notice made to the relevant persons in accordance with the obligation to enlighten shall be in clear, plain and simple language.

In case the personal data is not collected from the persons, the obligation to enlighten shall be fulfilled;

i. within a reasonable time after collecting the personal data,
ii. during the first contact if the personal data is intended for communication purposes with the relevant persons, and

iii. At the time of the initial transfer, at the very latest, if the personal data is to be transferred.

Communiqué on Procedures and Principles for Application to Data Controller (the "Application Communiqué")

The Application Communiqué was published in the Official Gazette No. 30356 dated March 10, 2018 and entered into force on the date of its publication. The Application Communiqué outlines the procedures of the application right of persons regarding personal data to the data controller and also the correspondence in between. There are certain requirements set forth in the Communiqué for the data controller in responding to these applications.

Persons can apply to the data controller concerning their rights stated in Article 11 of the Law through a variety of methods such as;

- a mobile application or software developed for the purpose of submission of these applications,
- through the e-mail address which is registered in the data controllers system and is previously notified by the persons to the data controller,
- Secured e-signature or mobile signature,
- In writing to the postal address or registered e-mail address (KEP) of the data controller.

The information which is mandatory to be included in the application made by the persons are;

- Name, surname and if the application is made in writing, the signature,
- Turkish I.D number or passport number together with nationality and identity number
- Residential or work address for notification.
- E-mail address (if any), telephone and fax number
- Subject to the demand regarding the application

The application date for the written applications will be the date when the application document is served upon the data controller or its representative. For non-written applications, the application date will be the date when the data controller receives the application.

The data controller is obliged to take every necessary administrative and technical measures effectively to finalize the aforesaid applications in accordance with the law and good faith. The data controller shall finalize the demands made in the application as soon as possible (according to the nature of the demand) and respond at latest in 30 days for free of charge. However, if the response is more than 10 pages, then the data controller can charge one Turkish Lira per page.

* * *

This newsletter has been prepared only for information purposes. Please do not hesitate to contact us if you need assistance or more detailed information.

Yours faithfully,
YAZICILEGAL