Building a better working world

Kuzey YMM ve Bağımsız Denetim A.Ş.
Eski Büyükdere Cad.
Orjin Maslak No:27
Maslak, Sarıyer 34398
İstanbul - Turkey

Tel: +90 212 315 3000
Fax: +90 212 234 1067
ey.com
Ticaret Sicil No : 479919
Mersis No: 0-6010-2772-0400010

A comparison of GDPR in European Union and Data Protection Law of Turkey

1. Introduction

In order to provide a more efficient protection for personal data and a high level of data protection within European Union ("EU"), General Data Protection Regulation ("GDPR") has been enacted by European Parliament as a result of long studies by repealing 95/46/EC numbered EU Data Protection Directive which was published in 1995.This new regulation increases the control of citizens over their personal data in the new digitalized world by means of social media, online banking, global transfers and smart phones. Hereby, the corporations which process EU citizens' personal data must be prepared for compliance and the countries must accord their legislations with the new regulation within 2 years.

2. Turkish Data Protection Law no. 6698

Protection of personal data means providing legal protection of data that belongs to a person and which can identify them. Personal data refers to any information relating to an identified or identifiable natural person such as name, surname, date of birth and place, telephone number, vehicle plate, resume, picture, IP address, hobbies, membership etc.

Processing of personal data

Processing of personal data means any operation which is performed upon personal data such as collection, recording, storage, preservation, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorization or blocking its use by wholly or partly automatic means or otherwise than by automatic means which form part of a filing system and the basic principles which must be regarded during the processing have been determined by the law. According to the law, personal data can only be processed by obtaining the explicit consent of the data subject as general rule being providing that the basic principles are regarded. Besides, it can be possible to process personal data without obtaining the explicit consent of the data subject if one of the exceptional condition exists.

Data controller and data processor

The law contains two separate notions as Data Controller and Data Processor. While data controller is defined as natural or legal person who determines the purposes and means of the processing of personal data, and who is responsible for establishment and management of the filing system, data processor is defined as natural or legal person who processes personal data based on the authority granted by and on behalf of the data controller.

3. GDPR innovations

Data Protection Officer

Data Protection Officer ("DPO") is located at the center of the compliance processes with GDPR for most of the organizations. GPDR obliges to appoint a DPO for data controllers and data processors. Basic duties of DPO can be determined as monitoring the order and systematic of data processing operations and executing the processes.

Audits

Data processor is liable for contributing the audits during the inspections conducted by data controller or an authorized auditor appointed by data controller. DPO, including relevant audits, shoulders the responsibility of monitoring the compliance of the policies of data controllers and data processor related to data protection with GPDR, other EU or member state data protection provision.

Data protection impact assessment

Data controller must conduct an impact assessment if the way of data processing contains high risk for rights and freedoms of real persons, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

Prior consultation

Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

Use of cookies

There is no any specific provision as to use of cookies under GPDR. Nevertheless, in GPDR, it has been stated that natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags.

Filing requirements

In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations. The records must include contact details of data controller, purpose of processing, description of data, transfers and receipts of data.

4. Comparison of GDPR and TDPL

Although TDPL is in compliance with European regulation to a large extent, there is still certain differences between Turkish and European legal acquis.

Scope of applicability

This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

On the other hand, TDPL applies to natural persons whose personal data are processed and natural or legal persons who process such data wholly or partly by automatic means or otherwise than by automatic means which form part of a filing system.

Rights of data subject

The rights of data subject under GDPR are stipulated as access, adjustment, to be forgotten, restriction of transactions, objection and data portability; the rights stipulated under TDPL are to learn whether or not her/his personal data have been processed, to request information as to processing if her/his data have been processed, to learn the purpose of processing of the personal data and whether data are used in accordance with their purpose, to know the third parties in the country or abroad to whom personal data have been transferred, to request rectification in case personal data are processed incompletely or inaccurately, to request deletion or destruction of personal data, to request notification of the operations to third parties to whom personal data have been transferred, to object to occurrence of any result that is to her/his detriment by means of analysis of personal data exclusively through automated systems, to request compensation for the damages in case the person incurs damages due to unlawful processing of personal data.

Administrative fines

The data subject must have the right to submit a complaint before regulatory body in case the regulation is violated while data processing. Depending on the type of violation, GDPR will apply such administrative fines:

a) up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher
b) up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher

While determining the fine, the nature, gravity and duration of the infringement, the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them will be regarded.

Asto the administrative fines stipulated under TDPL, to the ones who do not fulfil

a) Obligation to inform stipulated in article 10 of this Law, an administrative fine of 5.000 Turkish liras to 100.000 Turkish liras;

b) Obligations regarding data security stipulated in article 12 of this Law, an administrative fine of 15.000 Turkish liras to 1.000.000 Turkish liras;

c) Decisions of the Board as per article 15 of this Law, an administrative fine of 25.000 Turkish liras to 1.000.000 Turkish liras;

ç) Obligation to register with the Data Controllers Registry and notification stipulated by article 16 of this Law, an administrative fine of 20.000 Turkish liras to 1.000.000 Turkish liras

shall be imposed.

5. Conclusion

Considering the process in Europe, Data Protection Agreement has been issued in 1981 when transactions made by computers were increased, the framework has been prepared when in 1995 when internet has become widespread and GDPR has come into force in 2016 with the effect of social media development. As 1995 was only a framework and countries were enable to enact their own regulations freely within such framework, 2016 is a regulation with which compliance is an obligation. On the other hand, although DTP has been prepared in accordance with 1995, becoming law of the code can be regarded as another pave on the road of EU membership of Turkey.