Gap Analysis: General Data Protection Regulation versus Turkish Personal Data Protection Law

Abstract

General Data Protection Regulation ("GDPR")[1] is published on 8 April 2016 with intent to harmonize personal data protection legislation within European Union ("EU") and bring them in line with new, previously unforeseen ways that data is now processed by replacing Data Protection Directive (the "Directive")[2].

Its enforcement date is 25 May 2018 and by that date, all EU Member States need to be in line with the requirements/obligations set forth by the GDPR. However, compared to the Directive, GDPR sets up higher compliance requirements and stricter sanctions. Similarly, Turkish Personal Data Protection Law (the "Law")[3] lacks some of the improved, changed or newly added provisions, which might be problematic in an international level and/or in some cases may cause additional requirements for Turkish organizations wishing to process EU citizens' personal data.

In order to explain these contradictions; the main differences between GDPR and the Law is briefly explained below while GDPR's applicability to third country organizations is discussed in the beginning.

GDPR's applicability to third country organizations

In contrast to the Directive, GDPR not only applies to organizations established within EU, but according to article 3 of the GDPR, in some conditions, it may also apply to third country organizations that are processing EU citizens' personal data, where:

(i) an organization is ***offering goods/services directly to the EU citizens***, by directly addressing them, or ***clearly targeting them on its marketing campaigns/advertisements***, using EU currency even the currency is not used in the third country that the organization is established in;

(ii) an organization tracks EU citizens, profiles EU citizens or uses other monitoring techniques to monitor their behaviors.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016; on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. (General Data Protection Regulation)
[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995; on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[3] Turkish Personal Data Protection Law No. 6698.

Key differences between GDPR and the Law

The key differences between GDPR and the Law are listed*, inter alia,* below;

The term "pseudonym data" is not included in the Law. "Pseudonymisation" which refers to the technique of processing personal data in such a way that it can no longer be attributed to a specific "data subject" without using an additional information (pseudonym/key), which must be kept separately and be subject to technical and organizational measures to ensure non-attribution; is a term added to the data protection legislation by the GDPR.

Data subjects' right to data portability do not exist in the Law. In GDPR different from the Law, data subjects have a right to request their personal data to be transferred or directly transmitted from one data controller to another or receive a copy and/or store their personal data for further personal use on a private device in a structured, commonly used, machine-readable format that supports re-use.

The conditions of processing sensitive data without obtaining explicit consent are stricter under the Law. Different lawfulness basis of processing are set for sensitive personal data under GDPR compared to the Law such as; establishment, exercise or defense of legal claims, substantial public interest, vital interest, legitimate activities of non-profit bodies.

Data Protection Officer ("DPO") must be appointed and Privacy Impact Assessment ("PIA") must be conducted for some processing activates under GDPR. Unlike the Law, pursuant to article 37 of GDPR, controllers or processors must appoint a DPO if their processing activities involve regular and systematic monitoring of data subjects on a large scale or if they are processing sensitive personal data on a large scale. Where "high risk" processing will take place (such as monitoring activities, systematic evaluations or processing special categories of data) a detailed PIA must be undertaken and documented.

Unlike GDPR, "privacy by design" and "privacy by default" principles do not exist in the Law. "Privacy by design" creates a liability to take data protection risks into account and to take appropriate technical, legal and organizational measures to comply with GDPR accordingly. Besides, "privacy by default" requires controllers and processors to put appropriate mechanism in force to ensure that, by default, minimum amount of data is collected and processed according to its purpose of collection and also stored for a reasonable duration accordingly.

Administrative fines are noticeably higher in GDPR compared to the Law. As per to the article 83 of GDPR, the infringements of the provisions shall be subject to administrative fines 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. On the other hand, according to article 18 of the Law, the administrative fines are set between 5.000 TRY to 1.000.000 TRY.

GDPR enables more options for legally transferring personal data to third countries compared to the Law. GDPR and the Law both sets the following conditions as legal basis for data transferring with some differences:

- **Adequacy decision** taken by the European Commission (or by the Board in Turkey for transfers from Turkey), where the level of protection in the third country decided to be adequate;

- Providing **appropriate safeguards**; where under GDPR the safeguards are explained further as listed below:
    - Public authorities make **administrative arrangements** between themselves (Relevant Data Protection Authority ("DPA")'s approval is required if the arrangements include enforceable and effective data subjects' rights);
    - **Binding corporate rules** ("BCRs") are adopted within a corporate group to transfer personal data within the group, which includes members established in third countries as well, BCRs must meet the requirements set out under GDPR and **must be approved** by the DPA;
    - The controllers or the processors points out the safeguards taken by addressing the **Model Clauses**;
    - **Approved codes of conducts** or **certificates** if combined with binding and enforceable commitments of the data importer (additional DPA approval would not be needed);
- Controller adopting appropriate safeguards via **contractual clauses** which is subject to the Board's authorization (or contractual clauses (ad hoc) between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization approved by the relevant according to GDPR);

Further, Law also sets relevant Country's or the data subject's interest (where the relevant authorities and the Board's authorization of the transfer will still be sought) and provisions set forth by other laws regarding personal data transfer as legal basis for national personal data transfers; where different than the Law, GDPR sets the following as legal basis for not national but cross-border personal data transfers:

- Existing **judgement from a third country** where a specific data transfer could be allowed;
- The transfer is necessary for the **performance of a contract between the data subject and the controller** or the implementation of pre-contractual measures taken at the data subject's request;
- Necessity of the transfer for the **implementation of pre-contractual measures taken in response to the data subject's request** or **conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person ;**
- Necessity of the transfer for important reasons of **public interest**;
- Necessity of the transfer for the establishment, exercise or defense of **legal claims**;
- Necessity of the transfer in order to protect the **vital interests of the data subject or of other persons**, where the data subject is physically or legally incapable of giving consent;
- Transfer of personal data from a **public register** (not the entire register) which according to Union or Member State law is intended to provide information to the public and which

is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest;

- Non-repetitive transfer, concerning only a limited number of data subjects, and necessary for the purposes of **compelling legitimate interests pursued by the controller** which are not overridden by the interests or rights and freedoms of the data subject, where the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided appropriate safeguards with regard to the protection of personal data and informed the relevant DPA.

Umurcan Gago, LL.M.
Partner, Attorney at Law
T: +90 (212) 326 6472
umurcan.gago@gsghukuk.com

Alper Onar, LL.M.
Senior Manager, Attorney at Law
T: +90 (212) 326 6311
alper.onar@gsghukuk.com

Pınar Tatar, LL.M.
Manager, Attorney at Law
T: +90 (212) 326 6671
pinar.karamahmutoglu@gsghukuk.com