GÜN + PARTNERS
AVUKATLIK BÜROSU

Turkey is welcoming the long awaited Data Protection Law

While the world was adopting a data-driven economy, Turkey lacked a separate legislation on data protection. Enactment of a data protection law was a real need for Turkey's EU harmonization process since in the absence of such a regime, Turkey is found to be not adequate in terms of data protection standards. Although enactment of Turkish data protection law used to be on the agenda o the government for long time, it could not come into force until this year. Finally, Law on the Protection of Personal Data numbered 6698 (the "Law") was enacted as of April 07, 2016.

The Law, that is very much in line with the EU Directive 95/46/EC, contains detailed provisions relating to the protection of personal data, an area that was previously only covered by insufficient and piecemeal applications of different legislative measures and the general rules of the Turkish Constitution.

Personal Data and Personal Data of Special Nature

The Law introduces an official definition for the term "personal data", defining it as **"any type of information that relates to an identified or identifiable natural person"**. In this sense, ongoing controversies relating to legal entities and their data has been put an end it is determined that personal data can only relate to natural persons. The Law provides a definition that is parallel to the applicable EU measures, though one that is slightly less detailed.

The main principle is that personal data can only be processed once the data subject has provided explicit consent. However, if at least one of the following exceptions exists, personal data can be processed without obtaining explicit consent;

- The processing is **clearly mandated by Laws,**
- For a person who is unable to express their explicit consent due to a situation of impossibility, the processing is required for the safeguarding of their or a third person's life or physical wellbeing,
- The processing is **directly** related to the formation or execution of an agreement to which the data subject is a party,
- Processing is required for the data controller to **satisfy their legal obligation,**
- The data to be processed has been made public by the data subject,
- Processing is mandatory for the **establishment, use or protection of a right,**
- On the condition that it does not harm the data subject's fundamental rights and freedoms, the processing is mandatory for the **legitimate interests** of the data controller.

The Law also separately distinguished a category of "personal data of a special nature" which is subject to a more extensive level of protection. The types of personal data that fall under this category are related to race, ethnicity, political views, philosophical belief, religious denomination or other beliefs, clothing and attire, membership in associations, charities or trade unions, health, sex life, convictions, security measures and biometric data. The law-maker has set the standard of prohibition of processing personal data of special nature, unless explicit consent of the data subject is present.

However, in the situation where at least one of the following exceptions exists, there is no longer a requirement for explicit consent;

- Excluding health and sex life data, the processing is clearly mandated by law,
- Regarding sex life and health data, the data is to be processed by persons or authorized institutes bound by the duty of confidentiality for the purpose of the protection of public health, the provision of medical, diagnostic and treatment services and the planning, managements and financing of healthcare services.

By setting an additional level of protection, the Law dictates that personal data that falls under this category can only be processed if the sufficient precautions stated by the to-be-formed Data Protection Institution are adhered to.

Therefore, the current standard operating procedures regarding data protection in Turkey must be reviewed by each company engaging in such activities – particularly if the scope of processing cannot be said to fall under any of the aforementioned exceptions.

Data Protection Institution and Data Controller Registry

The Law provides for the incorporation of the Personal Data Protection Institution ("Institution") within six months from its enactment. The Institution will be positioned under the Prime Minister's office and shall be primarily responsible of enforcing the Law. Further, a Register of Data Controllers will be established and maintained by the Institution. Data controllers are required to be registered to the Register of Data Controllers before processing personal data. The registration will include, among others, information on the measures taken for ensuring data security, the data which will be transferred to third parties and/or other countries and the maximum period of retention needed for the process of personal data.

The obligation regarding the registration to the Register of Data Controllers will enter into force after six months from the enactment of the Law.

Transfer of Data

Articles 8 and 9 of the Law contain provisions relating to respectively the general transfer of data to third parties and the transfer of data abroad. With regard to the transfer of data to third parties, the main principle remains that explicit consent is required. However, in the exceptional situations set out above for the process of general personal data, personal data may be transferred without obtaining explicit consent whereas for personal data with special nature, the situations set out above for the process of personal data with special nature shall apply as an exception to explicit consent, provided that sufficient precautions are in place.

For transfer of personal data abroad the explicit consent of the data subject is required. Again however, if the exceptional situations set out above exist, the transfer of the data abroad may only take place if the foreign country has sufficient safeguards or, if they do not have such adequate safeguards, the data controller in the foreign country, must undertake to the Institution an adequate protection in writing for equivalent safeguards and the approval of the Institution must be obtained. Countries that have sufficient safeguards are to be determined by the Institution and a list of these countries will be published.

As the Institution is to be established within six months as of the Law coming into effect and as the provisions relating to transfer of data to third parties and abroad will also only come into effect at that time, it is not possible to comment as to how countries providing adequate protection will be designated but EU countries will be likely held within those with adequate protection.

Last but not least, as a result of long discussions at the Parliament, the Law includes a provision indicating that personal data can be transferred abroad in cases where the interest of Turkey or the data subject can be adversely affected, provided that the approval of the Institution is obtained, notwithstanding international treaties.

The Primary Obligations of the Data Controller

The Law introduces obligations on data controllers to ensure that personal data is processed and transferred lawfully and proportionally. The most important of these obligations are the requirements to inform the data subject, and to erase, destroy or anonymize personal data that has surpassed its purpose of processing.

The data controller's obligation to inform the data subject should be particularly taken into account while drafting the consent forms and agreements that are to be presented to the data subject. The scope of this obligation covers providing information on the identity of the data controller, the purposes of data processing and data transfer, the legal justification behind data collection, methods of collection of personal data, and the rights of the data subject. These are granted by the Law in relation to the right to request information on whether personal data is being processed or not, whether data is being transferred to third parties and details on those third parties and the purpose of the data controller in processing personal data. The data subject also has to request compensation for the damages they have suffered due to unlawful process of their personal data and to object to the conclusions that are to the detriment of the data and that are reached through the process of personal data by automatic means.

The rights granted to data subjects shall enter into force after six months from the enactment of the Law.

Data Controller's Obligation to Ensure Data Security

The Law further provides for data security obligations for data controllers and stipulates that data controllers are under the obligation to implement all kinds of technical and administrative measures to maintain a security level that would avoid unlawful processing of and access to personal data, whilst also safeguarding personal data. With the Law, it is clearly regulated that the data controller and the subcontractor and/or the data processor that process data on behalf of the data controller are jointly liable for maintaining the security measures. Although it is not clearly mandated by the Law, this provision signals out that it is beneficial for entities to have written agreements with their processors and outsource service providers, careful drafting of the recourse.

It should also be noted that the data controller has a duty to inform the Data Protection Board ("Board") and the relevant party if and when personal data has been unlawfully accessed. Thereafter, the Board has the discretion to announce the breach on its website or another via another communications channel.

Administrative Sanctions

In addition to criminal sanctions stipulated under the Turkish Criminal Code and repeated under the Law once again, the Law introduces administrative sanctions.

As per Article 18 of the Law, data controllers may face administrative monetary sanctions between the range of TRY 5,000 (approx. EUR 1,500) and TRY 1,000,000 (approx.EUR 300,000). Sanctions are specifically regulated for data controllers that are in breach of their obligations to inform the data subject, to ensure data security, enforce the decisions of the Board and to register to the Register of Data Controllers.

These sanctions shall enter into force after six months from the enactment of the Law. The important matter here is that the current provisions of the Turkish Criminal Code imposing criminal sanctions will be also be suspended for a period of 6 months as of the enactment of the Law.

Transition Period

Under the Law, there is a transition period for two years meaning that personal data that has been processed prior to the enactment of the Law must be brought in compliance with the provisions of the Law within the said period. In case such compliance is not ensured, incompliant personal data will be deleted, destroyed or anonymized. However, personal data for which the consents obtained legitimately before the enactment of the Law from the data subjects will be held compliant with the Law unless contrary statement is obtained from the data subject within 1 year.

In addition, for those data subjects' consent that were legitimately obtained shall be deemed to be in compliance with the Law, unless otherwise is communicated by the data subject.

As the Institution is currently being established and as the regulations that detail the application of the Law will be published within a one-year period, there is currently minimal guidance as to regional requirements that may be required for Turkey. It is currently not clear how the companies can adapt themselves to the Law and ensure all personal data obtained will be brought in compliance or how personal data will be deleted, destroyed or anonymized. It is expected that guidelines will be prepared by the Institution.

What to do now?

To say the least, the questions below must be evaluated with scrutiny by Turkish companies as well as foreign companies doing business in Turkey in the first place:

- What kind of data I am processing? Do those include personal data or personal data with specific nature?
- From which resources I am gathering data?
- For what purposes I am processing data?
- Which departments/units are engaged in the process of such data?
- What kinds of technologies are used?
- With whom such data is being shared?
- Where will I store the data?
- Will the data be transferred?
- Who are my business partners/subcontractors in processing such data?
- Am I subject to specific regulatory legislation which requires me to process personal data?

Thereupon, let the compliance process begin!

Begüm Yavuzdogan Okumus
Managing Associate

Bentley James Yaffe
Associate

Bensu Aydın
Associate

Gün + Partners

Esentepe Mah Kore Şehitleri Cad No. 17 34394 Istanbul Turkey
Tel: +90 212 354 00 00 Fax: +90 212 274 20 95
www.gun.av.tr