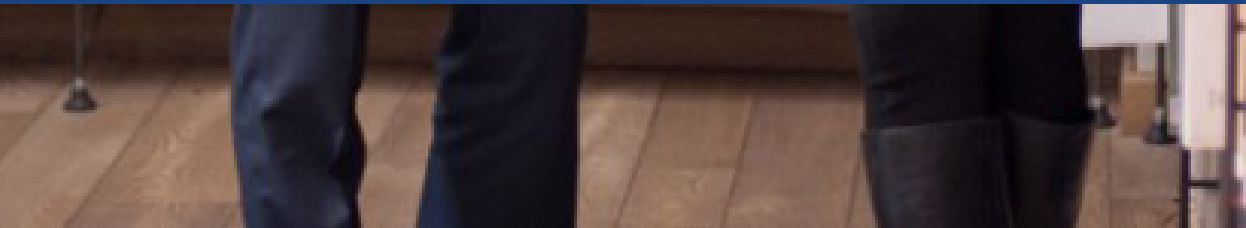
GÜN + PARTNERS
AVUKATLIK BÜROSU

DATA PROTECTION AND PRIVACY LAW IN TURKEY

KEY DEVELOPMENTS AND PREDICTIONS - 2020



FIRM OVERVIEW

We are one of the oldest and largest business law firms in Turkey and are ranked among the top tier legal service providers. We are widely regarded as one of the world's leading IP law firms.

Based in Istanbul, we also have working and correspondent offices in Ankara, Izmir and all other major commercial centers in Turkey.

We advise a large portfolio of clients across diverse fields including life sciences, energy, construction & real estate, logistics, technology media and telecom, automotive, FMCG, chemicals and the defence industries.

We provide legal services mainly in Turkish and English and also work in German and French.

We invest to accumulate industry specific knowledge, closely monitor business sector developments and share our insight with our clients and the community. We actively participate in various professional and business organisations.

Key Developments and Predictions for Data Protection and Privacy Law in Turkey

In this year's report, we focus on the key aspects of data privacy matters and developments in Turkey, and the most important or challenging issues regarding the same. The Data Protection Law entered into force in 2016. Even prior to its enactment, and afterwards, we have been dealing with privacy law and data protections issues.

We have seen a significant number of data breach decisions issued by the DPA in the last 2 years, and these shed a light on the practice and claims made at the level of DPA, which has also increased dramatically as stated by the DPA experts.

On the other hand, data breaches that have created global ambiguity have also been under the radar of the Turkish DPA. Sanctions imposed by the DPA have reached a noticeable number and, therefore, privacy issues has been at the top of the list of the agenda of most companies (local or global) providing goods/services in Turkey. Both local and global companies (to name a few - Amazon, Facebook, Zynga and Marriott) have had administrative fines imposed upon them by the Turkish DPA.

The Turkish DPA recently published an announcement on the importance of the right to be forgotten principle. Despite all the developments, the most debated issues in data privacy in Turkey remain as (i) data transfers outside of Turkey in the absence of a safe country list, (ii) processing of health data and the legal grounds of such processing, and (iii) controversial regulations regarding the judicial review of DPA decisions.

This paper provides an overview on the following topics:

- Data Protection Law in General
- Application of the Data Protection Law
- Lawful Data Processing
- Explicit Consent under Data Protection Law
- Transfer of Data to Third Party
- Transfer of Data Abroad
- Data Breach Notification
- Data Controllers' Registry (VERBIS)
- Consequences of Data Breach

Data Protection Law in General

On April 7, 2016, a new law on the protection of personal data came into force in Turkey: The Law on the Protection of Personal Data numbered 6698 ("Data Protection Law"). It is the first law of its kind in Turkey, specifically regulating the protection of personal data.

The Data Protection Law is a step towards harmonizing Turkish legislation with EU legislation, and it was prepared based on Directive 95/46/EC on data protection ("Data Protection Directive"). The Data Protection Law is very similar to the Data Protection Directive, but it is not a complete replica and, in relation to the Data Protection Law, some of the differences between them may be seen as deficiencies rather than improvements.

Since the enactment of the Data Protection Law:

- The Personal Data Protection Board ("Board") was established;
- A number of guidelines were issued in relation to the various concepts set out in the Data Protection Law;
- Various regulations and communiqués (that is, secondary legislation under Turkish law) were prepared by the Board and came into force in 2017 and 2018. The most notable ones among those regulations and communiqués are the following:
  - Regulation on Data Controllers' Registry;
  - Regulation on Erasure, Destruction and Anonymization of Personal Data;
  - Regulation on Working Principles of the Data Protection Board;
  - Communiqué on the Obligation of Information.

  The DPA issued various guidelines in order to provide insight on different matters. The most notable ones have been:
  - Guideline on Personal Data Security (Technical and Administrative Measures);
  - Guideline on Erasure, Destruction and Anonymisation of Personal Data;
  - Guideline on Preparation of the Data Inventory;
  - Guideline on Implementation of the Obligation to Inform.
- The DPA issued data breach decisions and principal decisions; and
  Data breach notifications have been made to the DPA and they were made public.

The DPA regularly publishes decisions and principle decisions that provides clarity to certain issues and outlines procedures for data breach incidents. We closely monitor the decisions of the DPA, as well as foreign data protection authority decisions for issues we need clarification of, and actively attend DPA workshops, or organize workshops, where practitioners and DPA experts come together to discuss the application of the Data Protection Law.

Application of the Data Protection Law

The Data Protection Law applies to data controllers who process and transfer personal data under their control. Furthermore, in the situation where data controllers utilise the services of third party data processors for these processes, the law holds them jointly liable for taking all of the technical and administrative measures required to ensure the safeguarding of personal data and to prevent any unlawful access or processing.

The Data Protection Law does not envisage the scope of its application in terms of territory. However, the DPA has the GDPR approach, and takes the view that the Data Protection Law is applicable to data controllers in Turkey, as well as data controllers not residing in Turkey, but who target data subjects in Turkey (monitoring and providing services and/ or goods in Turkey) irrespective of citizenship. The Data Protection Law does not aim to apply to those who are resident abroad, not targeting data subjects in Turkey but, randomly, may be in a position to provide goods/ services to persons in Turkey (passively).

The Data Protection Law does contain a provision that identifies areas exempted from its application, as follows:

- Use of personal data by real persons within the scope of activities relating to either themselves or their family members living in the same household, on the condition that the data is not provided to third parties and data security requirements are followed;
- Processing of personal data for official statistics or, on the condition that the data is made anonymous, used for purposes such as research, planning or statistics;
- On the condition that such use is not contrary to national defence and security, public safety and order, economic security, the right to privacy and personal rights, and, on the condition that it does not constitute a crime, processing for the purposes of art, history, literature or scientific research or processing within the scope of the freedom of speech;
- Processing within the scope of the preventive, protective, and intelligence activities of the public bodies and institutions that have been authorised by law to safeguard the national defence, security, public safety and order or economic security; or
- Processing by judicial authorities or penal institutions in relation to investigations, prosecutions, trials or enforcement proceedings.

We provide legal assistance to global companies having activities in Turkey, whether they have establishments in Turkey or not, we evaluate their activities, and advise on the procedures they need to follow as per the Data Protection Law.

Lawful Data Processing

Processing Personal Data

In principle, personal data can be processed with the explicit consent of the data subject. On the other hand, personal data can be processed without explicit consent in the following circumstances:

- If processing is clearly proposed under the laws;
- If processing is mandatory for the protection of life, or to prevent the physical injury of a person, in cases where that person cannot express consent, or whose consent is legally invalid due to physical disabilities;
- If processing is necessary for and directly related to the establishment or performance of a contract, and limited to the personal data related to the parties to the contract;
- If processing is mandatory in order for a data controller to fulfil its legal obligations;
- If the data is made manifestly public by the data subject;
- If processing is mandatory for the establishment, exercise, or protection of certain rights; and
- If processing is mandatory for the legitimate interests of the data controller, provided that fundamental rights and freedoms of the data subject or any related person are not compromised.

Processing Sensitive Personal Data

The Data Protection Law divides sensitive personal data into two categories:

- Personal data on health or sexual orientation; and
- "Other" sensitive personal data.

Personal data related to health or sexual orientation is protected more strictly than other sensitive data, as the scope of the additional legal grounds for processing is very limited. Reserving the requirement to obtain explicit consent of the data subject, personal data related to health or sexual data can only be processed by persons under an obligation of confidentiality, or by authorized institutions and establishments, for the purposes of protection of public health, protective medicine, medical diagnosis, treatment and care services.

For other types of sensitive personal data, these can only be processed with the explicit consent of the data subject, or if such processing is required by law.

Processing sensitive data, especially health data must be diligently handled in Turkey under the current legal backdrop. We have specific industry knowledge in health care where we frequently advise our clients in processing health data in different fields and for various purposes, including new technologies, quality services, pharmacovigilance or clinical trials.

Explicit Consent under Data Protection Law

Explicit consent has been defined as consent that relates to a specified issue, declared by free will and based on information.

The definition provides that not all kinds of consent will suffice under the Data Protection Law. The data subject must know for what he/she is providing consent, and must express his/her consent clearly. For example, consent obtained in English from non-English speakers in Turkey would not be considered to be explicit consent. Further, implied consent is not regarded as lawful under the Data Protection Law. However, the Data Protection Law does not envisage any form requirement to obtain consent from data subjects. Therefore, there is no need to collect explicit consent in writing, but on-line mechanisms will also be sufficient.

The explicit consent necessitates informing data subjects of the identity of the data controller, the purpose of the data processing, the persons to whom the data will be transferred, and for which purposes, the method and legal grounds for the collection of personal data, as well as the rights of the data subject. Therefore, consent mechanisms must be accompanied with information on data processing to be held valid.

Consent may be obtained for a specific purpose. Consent that is to be obtained for a vague or general purpose is not considered to be valid. Consent must be freely given; therefore, employee consent mechanisms must be handled very diligently.

Data subjects may withdraw their consent at any time during the data processing. Upon withdrawal of consent, data controllers cannot continue data processing in principal; however, exceptions to this principle exist exceptionally for certain sectors.

Transfer of Data to Third Party

Sensitive and non-sensitive personal data can be transferred to third parties if the explicit consent of the data subject is obtained, or if one of the additional legal grounds is applicable for such transfer.

The Data Protection Law does not provide a definition for a third party; therefore, any individual or entity (other than the data controller and the data subject) may be considered a third party. This creates a problem, especially in relation to transfers between data controllers and data processors, as there is no explicit provision in relation to data transfers between data controllers and data processors. As a result, any transfer of personal data from a data controller to a data processor may be interpreted as a transfer to a third party. Such an interpretation means that any such transfer would need to be made either:

- With the explicit consent of the data subject; or
- Where additional legal grounds exist.

"Data processor" is defined under the Data Protection Law as the natural or legal person who processes personal data on behalf of the data controller upon his/her authorization. As the data processor is an individual or a legal entity processing personal data "on behalf of" the data controller, it can be stated that the data processor is different from an ordinary third party. It acts under the authority of the data controller, making the data processor a part of the data controller's organisation. As the transfer of personal data between the employees of a data controller cannot be considered a transfer to a third party (although the data controller and each employee is a separate person), the transfer to the data processor should also not be considered as a transfer to a third party. This is a far-reaching interpretation, but if the Board adopts a decision in this respect, such an interpretation would be strong, and its chances of holding out against the test of a court would be high.

Transfer of Data Abroad

Sensitive and non-sensitive personal data can be transferred abroad if the explicit consent of the data subject is obtained.

Furthermore, other legal grounds will also apply to the transfer of personal data to the foreign country. However, the destination country must have "sufficient protection" in order to conclude the transfer abroad based on legal grounds (except for having obtained explicit consent). A list of jurisdictions that provide sufficient protection is to be determined by the Board. It has been confirmed by the DPA that they have been working on the issue of transfer to a foreign country; however, we do not expect the issuance of a safe country list in the near future, as the Board depends on the rule of reciprocity.

Pursuant to the Data Protection Law, if there is no sufficient protection in the destination country, for realisation of the data transfer, both:

- The data controller in Turkey and in the foreign country must provide a written commitment, stating that sufficient data protection will be provided; and
- The transfer must be authorised by the Board.

However, we have seen that obtaining a permit from the Board upon submitting a written commitment is not a clear process, and there is no predictable timeline as to when the parties may reach such a permit from the Board. Thus, making an application to the Board through submission of commitments in and of itself, or submitting intercompany transfer agreements, are not considered to be adequate.

As an alternative method for the transfer of data between multinational group companies where there is no sufficient protection in the destination country, the DPA introduced the concept of Binding Corporate Rules ("BCR"). Accordingly, BCR may be submitted to the DPA, and DPA's approval must be obtained to transfer personal data legally, without the need to obtain explicit consent (in cases where processing of personal data may be made based on legal grounds other than explicit consent, i.e. execution of the agreement, exercise of legal rights, or fulfilling legal requirements…etc.).

Data Breach Notification

The Data Protection Law requires data controllers to notify the relevant data subject and the Board as soon as possible when being made aware of such data breach. In its decision dated January 24, 2019 and numbered 2019/9, the Board clarified the rules and procedures to be applied in data breach incidents.

The Board takes the GDPR approach in terms of timing of breach notifications, and clarified that the term of "as soon as possible" must be interpreted as 72 hours of becoming aware of a data breach.

The Data Protection Law also requires data controllers to make notification to data subjects once they identify the data subjects being affected by the data breach, regardless of the fact of whether the risk of being negatively exposed is low or not.

The decision of the Board requires data controllers to prepare a road map in order to be prepared for data breaches, in advance, to clarify internal reporting mechanisms and procedures to be followed, in advance. The data controllers are obliged to keep record of data breaches and measures taken.

The data breach notification obligation also applies to data controllers residing abroad. If data controllers abroad experience a data breach incident, and such data breach affects data subjects residing in Turkey, and the services/ goods are used by data subjects in Turkey, then the data controllers abroad must also follow the data breach notification procedures announced by the Board.

The Board also published a "Data Breach Notification Template Form" for data controllers to complete while notifying the DPA. The DPA has also recently announced the online system to be used for notification of data breaches.

This subject has been a hot topic for privacy practitioners in Turkey. It has been observed that the DPA mostly issues fines upon the notifications of breaches made by companies. Some of the European Data Protection Authorities may have a more lenient approach towards breach notifications but, in Turkey, in most cases, the DPA issues a relevant fine upon receipt of notification.

Data Controllers' Registry (VERBIS)

Pursuant to Article 16 of the Data Protection Law, an obligation to register in the Data Controllers Registry has been introduced for data controllers.

In 2018, the Board issued decisions granting exemptions from registration obligation to certain professional groups, associations and political parties. The Board also granted a general exemption to local data controllers that have less than 50 employees, and actively less than TRY 25 million on their balance sheets.

Data controllers residing abroad are also required to be registered with the Data Controllers' Registry so long as they process personal data in Turkey.

The most important obligation regarding the Data Controllers' Registry is that a data controller must prepare a personal data inventory before registering; in other words, a type of data mapping of the data controller.
Every data controller must make a thorough review of its activities, determine the purposes of the processing activity, category of personal data, the recipients, retention periods, international transfers, data security measures, and legal grounds for data processing, while preparing data inventory.
Data controllers residing in Turkey must appoint a contact person. It is important to note that the Turkish subsidiaries of foreign companies must also appoint a contact person if such subsidiaries process personal data (however minimal their workforce in Turkey is). This individual's name and contact details will be published online, and they will be responsible for establishing the communication between the data subjects and the data controllers.

Furthermore, data controllers residing outside of Turkey must appoint an authorised representative. The representative may be either a legal entity or an individual. The appointment of the representative must be made with a resolution of the data controller, which needs to be notarised and apostilled (or otherwise legalised). The representative will act as a point of contact for the data controller in relation to its dealings with the Board, the DPA and the data subjects. If a legal entity is appointed as the representative, a real person must also be appointed by the foreign data controller as the contact person.

Data controllers who do not fulfil the obligation to register with the Data Controllers Registry will be sentenced with an administrative fine of between TRY 36,050 and TRY 1,802,640. (Based on the updated amounts of 2020.)

Consequences of Data Breach

The Data Protection Law envisages both administrative fines and criminal liability.

With regard to criminal penalties, the Data Protection Law refers to the relevant provisions of the Turkish Criminal Code that detail sanctions for the unlawful recording or accessing or transfer of personal data.

In addition to criminal sanctions, the Data Protection Law also contains provisions detailing administrative fines that are to be applied in the event of a breach. There are four main breaches that have been defined under the Data Protection Law:

(i) The data controller does not satisfy his/her obligation to inform the data subject;

(ii) The data controller does not satisfy the data security requirements;

(iii) The data controller does not implement the decisions of the DPA; and

(iv) The data controller does not satisfying the registration obligation with the Data Controllers' Registry.

These breaches can be sanctioned with administrative fines ranging from TRY 9.012 to TRY 1.802.640. (Based on the updated amounts of 2020.)

The DPA has issued numerous decisions for breach of the Data Protection Law, and imposes administrative fines on data controllers for not taking data security measures in cases where there is unlawful data processing or data transfers.

It has been observed in some cases that the DPA renders decisions where it applies fines upon a data breach notification or upon ex officio investigations without requesting further information and defences on the matter. Although the Regulation on Working Procedures and Principles of the Personal Data Protection Board does not explicitly require the Board to grant a right of defence to investigation subjects, such steps would enable a clearer justification for fines.

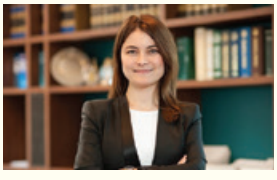
Although the Turkish courts have not effectively applied the Data Protection Law yet to impose criminal liability, the lack of expertise in the criminal courts in terms of data protection rules imposes a risk on data controllers and their data processing activities.

KEY CONTACTS

FİLİZ TOPRAK ESİN
PARTNER

Data Protection and Privacy
Business Crimes and Anti-Corruption
Competition
Corporate and M&A
Life Sciences

filiz.toprak@gun.av.tr



BEGÜM YAVUZDOĞAN OKUMUŞ
MANAGING ASSOCIATE

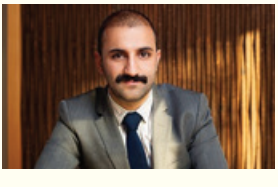
Data Protection and Privacy
Corporate and M&A
Technology, Media and Telecom
Life Sciences
Competition

begum.yavuzdogan@gun.av.tr

SELİN BAŞARAN SAVURAN
SENIOR ASSOCIATE

Data Protection and Privacy
Competition
Technology, Media and Telecom
Corporate and M&A
Life Sciences

selin.basaran@gun.av.tr



YALÇIN UMUT TALAY
SENIOR ASSOCIATE

Data Protection and Privacy
Corporate and M&A
Technology, Media and Telecom
Life Sciences

umut.talay@gun.av.tr

DATA PROTECTION AND PRIVACY

Our firm has a dedicated practice group for privacy and data protection law, and provides comprehensive services which cover not only personal data protection law issues (such as compliance, data protection advise, data subject rights and claims, international transfers, data localisation, sector specific rules and regulations, data beach notifications, and judicial remedies) but also transactions regarding data, i.e. license agreements, acquisitions, data use and data ownership matters.

We deal with all aspects of data protection law, including supervising and conducting data privacy compliance projects, advising multinational clients on a day to day basis. We work with both global and local data privacy teams and cooperate with them to ensure companies' compliance with the law.

We advise clients on their newly developed devices and prepare required policies and documents for relevant mobile applications or web sites.

We represent clients before the Turkish Data Protection Authority ("Turkish DPA" or "DPA") for notifications of breach and international transfer permit applications, including BCR approvals. Thanks to our in-depth experience in litigation, we provide clients with detailed appeal strategies to object to Turkish DPA decisions rendered against them. We represent clients before the Criminal Court of Peace to appeal decisions of the Turkish DPA. We also have a criminal lawyer assisting us in criminal proceedings.

We assist our clients to fulfil their Data Controllers' Registration obligations and represent them before the Turkish DPA. We act as representative for foreign data controllers who are subject to registration in Turkey.

We further provide advice on data localization issues specific to Turkey, and advise our clients in M&A projects regarding data transfers and data protection compliance matters.

Our industry strengths are life sciences especially in pharmaceuticals and medical devices, banking, technology, media and telecom.

GÜN + PARTNERS
AVUKATLIK BÜROSU

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: + 90 (212) 354 00 00
F: + 90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr