GÜN + PARTNERS
AVUKATLIK BÜROSU

DATA PROTECTION AND PRIVACY LAW IN TURKEY

KEY DEVELOPMENTS AND PREDICTIONS

2022

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, cyber security & incident response services and 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.

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

The Law on the Protection of Personal Data numbered 6698 ("Data Protection Law") entered into force in 2016. Even before its enactment, we have been dealing with privacy and personal data protection law, and we have further intensified and deepened our activities in this field with the enactment of the Data Protection Law. This year's report focuses on the key aspects of data privacy matters and developments in Turkey, and the most important or challenging issues regarding data privacy.

In 2021, we saw many data breach decisions issued by the Personal Data Protection Authority ("DPA"). These decisions have shed light on the practice and claims made at the level of the DPA, which also dramatically increased, as stated by the DPA experts.

On the other hand, data breaches that have created global attention have also been under the radar of the DPA. Sanctions imposed by the DPA have reached a noticeable number, and therefore, privacy issues have been at the top of the agenda of most companies (local or global) providing goods/services in Turkey. Decisions have been passed about many data controllers operating in the insurance, education, health and service sectors, and data controllers have issued data breach notifications. Both local and global companies (to name a few – Amazon, WhatsApp, Yemek Sepeti) have had administrative fines imposed by the DPA. The DPA has continued to avoid mentioning the companies about which decisions have been passed, yet it has disclosed some of them in certain decisions. The DPA's tendency not to announce reasoned/long decisions to the public and not to disclose identities of data controllers, as a rule, has drawn heavy criticism.

Among the outstanding decisions passed in 2021, WhatsApp and Yemek Sepeti decisions can be listed. At the beginning of 2021, the investigation launched into WhatsApp was concluded, and the Personal Data Protection Board ("Board") submitted a data breach decision against WhatsApp and imposed an administrative fine on the company. Within this scope, the importance of explicit consent for transferring personal data abroad and the requirement to obtain the relevant explicit consent in conformity with the law was noted. Also, it was underlined that explicit consent could not be presented as a precondition for providing services. Additionally, the Board made assessments regarding cookies for the first time in the referred decision. In Yemek Sepeti decision regarding the data breach, which resulted from the vulnerability of the web application server, it was noted that the data controller failed to notice the breach for eight days and was at fault in controlling which software and services were running on its information networks and in determining whether there was infiltration or an action that should not have occurred. Accordingly, the Board decided to impose an administrative fine on the company.

Within the scope of the judicial reform package, draft articles have been written down concerning the amendments which are planned to be made to Articles 6 and 9, namely the most disputed provisions of the Data Protection Law.

The DPA has published the Guideline on Things to Consider When Processing Biometric Data and Recommendations on The Protection of Personal Data in The Field of Artificial Intelligence the last year. The right to be forgotten by search engines has been assessed. Also, the Communiqué on the Procedures and Principles Regarding the Personnel Certification Mechanism has been published by the DPA. Even though the referred Communiqué was considered to be a positive development in terms of integration with the EU General Data Protection Regulation ("GDPR") upon its publication; with an announcement made by the DPA, it was stated that the institution regulated in the relevant Communiqué did not correspond to the Data Protection Officer, within the meaning of the EU Law.

In 2021, the DPA published the Draft Guidelines on Cookies Applications for the public's opinions and recommendations. Within the scope of the referred draft guidelines, types of cookies, conditions for data processing through cookies, examples of good and bad practices regarding how cookies checkboxes should be prepared were also published.

Finally, the DPA clearly defined the concept of "joint data controller" in the Board's decision published on January 20, 2022. This decision concluded that car leasing companies that use the blacklist application violate the laws in processing their customers' data. Transferring personal data that was processed without the consent of the data subject through an application with other car leasing companies was also against the law, and the car leasing companies which have the relevant data and software companies are joint controllers. The liabilities and negligence of joint data controllers shall be evaluated and determined on a case-by-case basis, considering the concrete circumstances of each case.

In this paper, wherein the developments seen in the field of personal data protection and privacy in Turkish Law within the last year have been reviewed; an overview on the following topics is provided:

- Data Protection Law in General
- Application of the Data Protection Law
- Lawful Data Processing
- Explicit Consent under Data Protection Law
- Transfer of Personal Data to Third Party
- Transfer of Peronal Data Abroad
- Data Breach Notification
- Data Controllers' Registry (VERBIS)
- Consequences of Data Breach
- Judicial Review of Board Decisions
- Planned Amendments to the Data Protection Law
- Draft Guidelines on Cookies Applications

Data Protection Law in General

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

The Data Protection Law is a step towards harmonising Turkish legislation with EU legislation, and it was prepared based on Directive 95/46/EC on data protection ("Data Protection Directive"). The Law is very similar to the Data Protection Directive, although it is not a complete replica. Furthermore, certain principles of the General Data Protection Regulation ("GDPR") were also considered in the preparation of the Law. On the other hand, some of the differences between the Data Protection Law and Data Protection Directive and the GDPR may be seen as deficiencies rather than improvements in the Data Protection Law.

Since the enactment of the Data Protection Law:

- The Board was established;
- Several guidelines were issued concerning the various concepts set out in the Data Protection Law;
- The board prepared various regulations and communiqués (secondary legislation under Turkish law) and put them into force. 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.
  - Communiqué on The Principles and Procedures for The Application To Data Controller.
- The DPA issued various guidelines 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 Processing Inventory;
  - Guideline on Implementation of the Obligation to Inform.
  - Guideline on Things to Consider When Processing Biometric Data.
- 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 clarify specific issues and outline procedures for data breach incidents. We closely monitor the DPA's and foreign data protection authority's decisions about issues we need clarification and actively attend DPA workshops or organise 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. 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 prevent any unlawful access or processing.

The Data Protection Law does not envisage the scope of its application in terms of territory. However, the Law has the GDPR approach in general and in this regard, it takes the view that the Data Protection Law applies to data controllers in Turkey, as well as data controllers not residing in Turkey, but who target data subjects in Turkey (in other words those monitoring and providing services or goods in or to 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, maybe in a position to provide goods/ services to persons in Turkey (passively).

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

- Use of personal data by natural 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 art, history, literature or scientific research or processing purposes 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 about investigations, prosecutions, trials or enforcement proceedings.

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

Lawful Data Processing

Processing Personal Data

Personal data can be processed based on the below specified legal grounds:

- If explicit consent of the data subject is obtained;
- 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 therein;
- If processing is mandatory 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 compulsory 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 process data by obtaining the 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 authorised institutions and establishments, for protection of public health, protective medicine, medical diagnosis, treatment and care services purposes.

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

In Turkey, processing sensitive data, especially health data, must be diligently handled under the current legal backdrop. We have specific industry knowledge in health care where we frequently advise our clients to process 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 s/he is giving consent and must clearly express his/her consent. 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 required to obtain consent from data subjects. Therefore, there is no need to collect explicit consent in writing, but online 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. A consent received for a vague or general purpose is not considered valid. It must be freely given; therefore, employee consent mechanisms must be handled 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 principle; however, exceptions to this principle exist exceptionally for specific sectors.

Aside from this, in the decisions concerning fitness centres, the DPA once again emphasised the requirement to comply with the principle of proportionality even in the presence of explicit consent and ruled that explicit consent will not be deemed valid legal grounds for data processing activities that are contrary to the principle of proportionality.

Transfer of Data to Third Party

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

The Data Protection Law does not define 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 about transfers between data controllers and data processors, as there is no explicit provision concerning 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 Protection Law defines a "Data Processor" as the natural or legal person who processes personal data on behalf of the data controller upon their authorisation. As the data processor is a natural person 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), then 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. However, under the current circumstances, each transfer made to a data processor is considered a data transfer to a third party.

Transfer of Data Abroad

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

Furthermore, other legal grounds will also apply to transferring personal data to a foreign country. However, the destination country must have "sufficient protection" 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. The DPA has confirmed that they have been working on the list of safe countries regarding the data transfer abroad, yet since the referred list is prepared based on reciprocity, for now, no foreign country has been announced to be safe by the Board.

According to the Data Protection Law, if sufficient protection in the destination country for the realisation of the data transfer does not exist, both:

- The data controller in Turkey and the foreign country must provide a written commitment, stating that sufficient data protection will be provided; and
- Authorisation must be obtained from the Board to transfer data to the relevant foreign country.

However, we have seen that obtaining a permit from the Board upon submitting a written commitment is not a transparent process, and there is no predictable timeline either 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, is not considered adequate. Also, it would be appropriate to note that a limited number of business enterprises have made such an application and obtained a permit to transfer data abroad.

As an alternative method for transferring data between multinational group companies where there is not sufficient protection in the destination country, the Board introduced the concept of Binding Corporate Rules ("BCR"). Accordingly, Binding Corporate Rules may be submitted to the Board, and the DPA's approval must be obtained to transfer personal data legally between multinational group companies, without the need to obtain explicit consent (in cases where the processing of personal data may be made based on legal grounds other than explicit consent, i.e. execution of the agreement, the exercise of legal rights, or fulfilling legal requirements, etc.).

The fact that there is currently no fast solution for the transfer of personal data abroad except for obtaining explicit consent, and that the legal instruments, such as standard contractual clauses, alone, are not adequate for the transfer of personal data abroad,

undisputedly reveals that an amendment to the Law must resolve this issue. It is expected to resolve this issue by taking concrete steps in the short term under the current legislation, as it also affects commercial relations. Within this scope, it is seen that certain amendments are planned to be made to Article 9 on the transfer of personal data abroad, as a part of the proposed amendments to the Data Protection Law, which the DPA has shared with stakeholders in the sector. Referred proposed amendments have not been finalised and enacted yet. However, it is a meaningful development in that the deficiency pointed out by us has also been accepted by the DPA, and they have been working to remedy it. Our assessments on the content of amendments are presented in the relevant section of this document.

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 applied in data breach incidents.

The Board took the GDPR approach in terms of timing of breach notifications and clarified that "as soon as possible" within the Data Protection Law must be interpreted as 72 hours from becoming aware of a data breach. The Data Protection Law also requires data controllers to notify data subjects once they identify the data subjects being affected by the data breach, regardless of whether or not the risk of being negatively exposed is low.

The decision of the Board requires data controllers to prepare a road map in the event of data breaches in advance and clarify internal reporting mechanisms and procedures to be followed in advance. Data controllers are obliged to record 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 used by data subjects in Turkeydata subjects in Turkey use the services/goods, 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 primarily issues fines upon the notifications of breaches made by companies. Some European Data Protection Authorities may take a more lenient approach towards breach notifications. However, it should also be noted that the Board has passed recent decisions wherein no administrative fines were imposed by considering the number of persons affected by the data breach, whether the violation in question has adversely affected the data subject or not, whether the data controller can interfere in, whether the data subject to breach is deleted, whether the data controller has notified the breach within the legal deadline, whether reasonable administrative and technical measures have been taken or not.

Data Controllers' Registry (VERBIS)

According 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 specific professional groups, associations, and political parties. The Board also granted a general exemption to local data controllers with less than 50 employees and less than TRY 25 million on their balance sheets.

Data controllers residing abroad must also 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 thoroughly review its activities and determine the purposes of the data 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 who reside in Turkey and meet the conditions above for registration obligation to the Data Controllers' Registry must appoint a contact person. It is important to note that the Turkish subsidiaries of foreign companies meeting the conditions mentioned above for registration to the Data Controllers' Registry must also appoint a contact person if such subsidiaries process personal data. 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.

On the other hand, data controllers residing outside Turkey must also appoint a data controller representative. The representative may be either a Turkish resident legal entity or a Turkish national individual. The representative must be appointed via the data controller's resolution, which needs to be notarised and apostilled (or otherwise legalised). The representative will act as a point of contact for the data controller about its dealings with the Board, the DPA and the data subjects. If a legal entity is appointed as the representative, the foreign data controller must also appoint a real person as the contact person.

Data controllers who do not fulfil the obligation to register with the Data Controllers' Registry will be sentenced to an administrative fine of between TRY 53,572 and TRY 2,678,859 (Based on the updated amounts for 2022). The DPA set the final date for registering with the Data Controllers' Registry as 31.12.2021, and no extension decision has been passed since the expiry of the prescribed deadline.

Consequences of Data Breach

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

Regarding criminal penalties, the Data Protection Law refers to the relevant provisions of the Turkish Criminal Code that detail sanctions for the unlawful recording, disclosing, or transferring of personal data.

In addition to criminal sanctions, the Data Protection Law also contains provisions detailing administrative fines applicable in a breach. Four violations have been defined under the Data Protection Law:

i. The data controller does not satisfy their 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 satisfy the registration obligation with the Data Controllers' Registry.

These breaches may be sanctioned with administrative fines ranging from TRY 13,391 to TRY 2,678,859. (Based on the updated amounts for 2022.)

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

In some cases, 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 more precise justification for fines.

It should also be noted that the DPA has started to issue decisions on its official website, beginning from the last months of 2021, where administrative fines are imposed.

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

Judicial Review of Board Decisions

The Data Protection Law does not include an explicit provision concerning the appeal process of Board decisions imposing administrative fines. However, it is accepted that criminal courts of peace are the authorised courts under Law No. 5326 on Misdemeanours dated 30/3/2005 since the title of Article 18 of the Data Protection Law is "Misdemeanours," and administrative fines are issued as per Article 18 of the Data Protection Law. With this in mind, decisions imposing behavioural sanctions can be appealed before administrative courts. This controversial issue is subject to discussions in practice and among academicians.

Criminal courts of peace are first instance courts in Turkey, and their decisions are subject to review of other criminal courts of peace which are, again, first instance courts. On the other hand, once the appeal process before the criminal courts of peace is completed, it is also possible to apply to the Turkish Constitution Court.

Criminal proceedings before the criminal court of peace require close follow up as the cases before the criminal court of peace are subject to simple legal proceedings, and the courts may resolve a decision quickly without a hearing. Therefore, in addition to having deep experience in data protection law, litigation experience with a criminal law background is of the essence. Thus, while representing our clients before the criminal court of peace for appeal of Board decisions imposing administrative fines, we created a team of lawyers who have legal expertise in privacy law matters and litigation and include criminal lawyers on our team in these cases.

Administrative courts are more capable and experienced to review administrative decisions when compared to criminal courts. We believe that the Board decisions, in general, must be considered as administrative decisions and must be subject to uniform judicial review so that each stakeholder may benefit from the in-depth analysis that can be made during judicial review and arguments made therein.

CONTACTS

BEGÜM YAVUZDOĞAN OKUMUŞ
PARTNER

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

begum.yavuzdogan@gun.av.tr

DİCLE DOĞAN
MANAGING ASSOCIATE

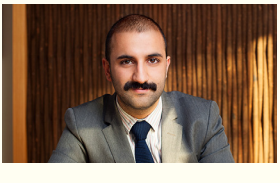
Data Protection and Privacy
Life Sciences
Intellectual Property
Trademarks and Designs

dicle.dogan@gun.av.tr

DİRENÇ BADA
SENIOR ASSOCIATE

Data Protection and Privacy
Dispute Management
Intellectual Property
Anti-Counterfeiting

direnc.bada@gun.av.tr



YALÇIN UMUT TALAY
SENIOR ASSOCIATE

Data Protection and Privacy
Corporate and M&A
Technology, Media and Telecom
Business Crimes and Anti-Corruption
Life Sciences

umut.talay@gun.av.tr

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 office 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 inn Turkish and English and also work in German and French.

We invect 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.

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