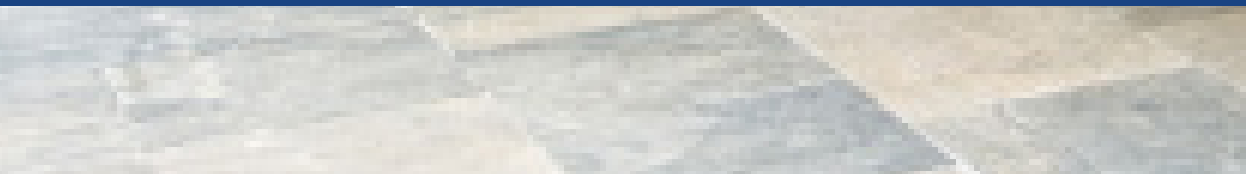
GÜN + PARTNERS
AVUKATLIK BÜROSU

DATA PROTECTION AND PRIVACY LAW IN TURKEY

KEY DEVELOPMENTS AND PREDICTIONS

2023



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

This year's report focuses on the basic regulations and principles of personal data protection law, developments in Turkey, and the most important or challenging issues regarding data privacy as well as the latest developments in the field of personal data protection, the latest decisions and published guidelines. The Law on the Protection of Personal Data numbered 6698 ("**Law**") entered into force in 2016. In 2022, it has been observed that settled case-laws have started to developin the personal data protection law, which went beyond the foundation provided with the Law, in accordance with new regulations and Personal Data Protection Board ("**Board**") decisions. Nonetheless, acts that constitute an element of crime have also been subject to jurisdiction within the scope of the regulations of Turkish Criminal Law regarding the protection of personal data. It has been observed that fundamental decisions have been made by the Constitutional Court in terms of the protection of personal data.

In brief, decisions were made regarding insurance, banking, health and service industries about several data controllers and data breach notifications were made by data controllers in 2022.

In 2022, as per the data notifications, Turkish Data Protection Authority ("DPA") showed its sensitivity regarding user data before *DPA with its Public Announcement on Technical and Administrative Measures Recommended to be Taken by Data Controllers Regarding User Security, published for the purpose of preventing the access to user account information used for logging in the websites of data controllers operating in finance, e-commerce, social media and online game sectors via security* vulnerabilities in data controllers' systems or in end-users' computers and preventing such common data breaches , or ensuring the mitigation of the possibility of negative outcomes on the data subjects in cases of such breaches.

The Regulation on Protection and Processing of Personal Data by the Social Security Institution was published regarding the processing of data obtained via automated or unautomated means within the scope of Social Security Institution's ("SSI") duties and authorities.

In addition, the *Guideline on Good Practices of the Protection of Personal Data in the Banking Sector* was published by DPA. In this guideline, banks are considered as data controllers in terms of the activities they carry out in accordance with article 4 of the Banking Law, the guideline also refers to the points to be included in the data processing contracts with regard to the relationship between the data controller and data processorand includes explicit consent, which is one of the conditions to process data and obligations of the banks that are data controllers . Subsequently, *the Regulation on the Collection, Storage and Disclosure of Insurance Data was* published for an area

where frequent and serious breaches are likely to occur. In this regulation, the concept of insurance term is defined with an extensive scope and it has been observed that those who keep insurance data are obliged to present the documents requested by the Insurance Information and Surveillance Centre, the Regulation explicitly defines the fundamental aims of the use of insurance data and the use specific to the Insurance Information and Surveillance Centre and introduces regulations regarding the requests for receiving information and data exchange in terms of insurance data.

For the first time, the Board issued a decision, which is about the processing of personal data via exclusively automated means and which evaluates profiling, evaluating the software used by rental companies and providing a black list and concluded that data was processed unlawfully and pointed out joint data controllership.

In a recent decision regarding the processing of biometric data, the Board reiterated its stance that this method should only be used on an exceptional basis by concluding that methods involving the processing of employees' biometric data cannot be used to control the entry and exit to work and to ensure occupational health and safety. It was particularly stated that processing biometric data for controlling entry and exit and ensuring occupational health and safety is not a proportionate practice and that these goals shall be achieved with alternative methods. It was decided to destroy the personal data and verification data obtained by facial recognition systems until the date of the decision. It has been observed that the Board has developed a case law on this subject.

Furthermore, considering the shortcomings in meeting the obligation to register to the Data Controllers' Registry ("VERBIS") due to pandemics, the time prescribed to complete the registry records in accordance has expired, and administrative fines have started to be imposed on data controllers who do not fulfil this obligation following the reminders in DPA announcements and the control of the records. It is stated that the amounts of administrative fines are estimated in accordance with the "Algorithm Table of Administrative Fine Amounts for Domestic Data Controllers".

The Board issued a decision imposing an administrative fine on the data controllers operating in the e-commerce sector who unlawfully process data using cookie applications. DPA announced the criteria and conditions for cookie applications and lawful data processing by publishing Guidelines on Cookies Application in June 2022.

In our report, which reviews the developments in the field of personal data protection and privacy in Turkish Law within the last year; also presents an overview on the following topics :

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

The Law on the Protection of Personal Data

On April 7, 2016, the Law on the Protection of Personal Data ("**Law**") came into force in Turkey as a special law regarding the protection of personal data.

The 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**"). Although the Law is very similar to the Data Protection Directive, certain principles of the General Data Protection Regulation ("**GDPR**") were also considered in preparing the Law. It can be argued that there are some fundamental issues that differentiate from the GDPR in terms of the application and wording of the Law, and it is crucial for foreign companies operating in Turkey to consider these differences.

Application of the Law on the Protection of Personal Data

The provisions of the Law apply 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 technical and administrative measures required to safeguard personal data and prevent any unlawful access or processing.

The 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 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 Law does not aim to apply to those who are residents abroad and do not target data subjects in Turkey but, randomly, might be in a position to provide goods/services to persons in Turkey (passively).

The circumstances excluded from the scope of the application of the Law are as follows:

- Processing 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.

Authors: Begüm Yavuzdoğan Okumuş, Umut Yalçın Talay, Seda Öztürk

Lawful Personal Data Processing

Personal data can be processed based on the following 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 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 the 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. The processing of health data in different areas and for various purposes, including new technologies, quality services, pharmacovigilance or clinical trials, are the areas where companies need to be careful in their data processing practices. Further, processing employee data must be diligently assessed and managed.

Authors: Begüm Yavuzdoğan Okumuş, Umut Yalçın Talay, Seda Öztürk

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.

As it can be understood from the definition, the Law stipulates that all kinds of consent not limited to a specific subject and not limited to the relevant transaction, also known as "blanket consents", will not be valid. For example, consent not limited to a specific subject and activity, such as "I allow all kinds of data processing activities", will not suffice under the 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 as an explicit consent. Since explicit consent must include the positive declaration of the data subject, implied consent is not regarded as lawful under the Law. However, the 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. 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.

Authors: Begüm Yavuzdoğan Okumuş, Umut Yalçın Talay, Seda Öztürk

Transfer of Personal Data to Third Parties

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 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.

The 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.

Authors: Begüm Yavuzdoğan Okumuş, Umut Yalçın Talay, Seda Öztürk

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). The Board will determine a list of jurisdictions that provide sufficient protection. The Board 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 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 the 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 applied and obtained a permit to transfer data abroad.

As an alternative method for transferring data between multinational group companies where there is insufficient 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 Board'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 Board has shared with stakeholders in the sector.

With the amendment in question, a three-step assessment system has been proposed for transferring data abroad. Within this scope, it will be evaluated firstly whether an adequacy decision has been issued specifically to the sector. In the absence of an adequacy decision held by the Board, personal data will be transferred if one of the appropriate guarantees has been given. Also, the Board may ask for other undertakings. In the absence of an adequacy decision and relevant undertakings provided by the data controller, personal data can be transferred abroad solely in the exceptional cases listed below, within the scope of the proposed amendment.

(i) Adequacy Decision

In the presence of the legal grounds outlined in Articles 5 and 6 of the Data Protection Law and upon issuance of an adequacy decision relating to the country, sector or international organisation within the country where the data is to be transferred (including onward transfers), personal data may be transferred abroad. The Board will grant an adequacy decision based on the reciprocity rule and consider other aspects.

(ii) Appropriate Undertakings

(i) In the absence of an adequacy decision issued by the Board, personal data can be transferred abroad provided that one of the following appropriate undertakings is granted by the data controller:

- Notification to the Board with a standard undertaking, which the Board has also published,
- Submission of a written agreement to the Board, including protective measures that will be applicable and obtaining the Board's permission,
- Presence of binding corporate rules and approval of the BCRs by the Board,
- Presence of provisions on the protection of personal data in agreements to be executed between the public entities and bodies in Turkey and the corresponding public entities and bodies in the foreign country where the personal data is to be transferred and obtaining the Board's permission.

Finally, in cases where an adequacy decision has not been issued or the data controller

does not provide related undertakings, it is proposed that data transfer will be made in exceptional cases based on the following conditions:

. (i) Upon explicit consent of the data subject after informing him/her about the potential risks originating from the absence of appropriate undertakings,

. (ii) transfer of personal data of the contracting parties is obligatory provided that such transfer is directly related to the establishment or performance of the contract,

. (iii) conclusion or performance of a contract that is executed for the benefit of this party data subject, under which transfer of the contracting parties' personal data is obligatory,

. (iv) data transfer is mandatory for the protection of the life or bodily integrity of a person who is incapable of giving consent or whose consent is not legally valid or of another person,

. (v) data transfer is obligatory for the establishment, exercise or protection of a legal right, and

. (vi) solely as a temporary case, transfer of personal data is obligatory to perform duties and powers of public bodies and organisations or professional institutions with public duties, as outlined in the relevant regulations.

Referred proposed amendments have yet to be finalised and enacted. However, it is a meaningful development in that the deficiency we pointed out has also been accepted by the Board, and they have been working to remedy it.

Authors: Begüm Yavuzdoğan Okumuş, Umut Yalçın Talay, Seda Öztürk

Data Breach Notification

The Law requires data controllers to notify the relevant data subject and the Board as soon as possible when being made aware of such a 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 regarding the timing of breach notifications and clarified that "as soon as possible" within the Law must be interpreted as 72 hours from becoming aware of a data breach.

The Law also requires data controllers to notify data subjects once they identify the data subjects 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 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 Board.

This subject has been a hot topic for privacy practitioners in Turkey. It has been observed that the Board primarily issues fine upon the notifications of breaches made by companies. 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.

Authors: Begüm Yavuzdoğan Okumuş, Umut Yalçın Talay, Seda Öztürk

Data Controllers' Registry (VERBIS)

According to Article 16 of the Law, an obligation to register in the Data Controllers Registry ("VERBIS") 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 data controllers residing in Turkey 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 VERBIS, so long as they process personal data in Turkey.

The most important obligation regarding the VERBIS 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, recipients, retention periods, international transfers, data security measures, and legal grounds for data processing while preparing data inventory.

Data controllers residing in Turkey and meeting the conditions above for registration obligation to the VERBIS 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 VERBIS 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 an individual with Turkish nationality. 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 VERBIS will be sentenced to an administrative fine of between TRY 119,436 and TRY 5,972,040 (Based on the updated amounts for 2023).

Authors: Begüm Yavuzdoğan Okumuş, Umut Yalçın Talay, Seda Öztürk

Consequences of Data Breach

The Law envisages both administrative fines and criminal liability.

Regarding criminal penalties, the 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 Law also contains provisions detailing administrative fines applicable in a breach. Four breaches have been defined under the 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 Board;
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 29,853 to TRY 5,971,980. (Based on the updated amounts for 2023.)

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

In some cases, the Board renders decisions where it applies fines upon data breach notification or ex officio investigation 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.

Although the Turkish courts have not yet effectively applied the 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.

Authors: Begüm Yavuzdoğan Okumuş, Umut Yalçın Talay, Seda Öztürk

Judicial Review of Board Decisions

The 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 Law is "Misdemeanours," and administrative fines are issued as per Article 18 of the 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 by 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 with legal expertise in privacy law matters and litigation and included criminal lawyers on our team in these cases.

Administrative courts are more capable and experienced in reviewing administrative decisions when compared to criminal courts. We believe that the Board decisions, in general, must be considered 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.

Authors: Begüm Yavuzdoğan Okumuş, Umut Yalçın Talay, Seda Öztürk

Guidelines on Cookies Applications

The Board prepared the Guidelines on Cookies Applications ("Guidelines") explaining cookies and practical advice for data controllers who process personal data through cookies. The Guidelines was published on the official website of the DPA on June 20, 2022.

Within the Guidelines, cookies in general and their types are regulated. Moreover, the types of cookies are categorised based on their timeframe, intended purpose and parties.

The relationship between the Electronic Communications Law No. 5809 ("ECL") and Data Protection Law is also reviewed in the Guidelines. Personal data may be processed without the need for explicit consent in cases where the cookies in question are solely used for communication via the electronic communications network, and the data controller acts as an operator within the meaning of the ECL. Within the scope of the Guidelines, in respect to cookies applications, it is stated that the Data Protection Law shall be applied, and the principles outlined in the Data Protection Law and the grounds for processing data shall also apply to the processing of personal data through cookies other than the exceptional cases, listed above and subject to the provisions of the ECL. Accordingly, in the absence of the legal grounds listed in Articles 5 and 6 of the Data Protection Law, explicit consent from website visitors shall be obtained for using cookies.

Within the framework of the Guidelines, in cases where cookies are solely used to provide communication via the electronic communications network (Criteria A) or the use of cookies is essential for the member or the user to receive the service that they have explicitly demanded (Criteria B), cookies may be used without the need for obtaining explicit consent if it is mandatory for the legitimate interests of the data controller as outlined in subparagraph (f) of Article 5 of the Data Protection Law. No restriction has been introduced in the Guidelines regarding the grounds outlined in Articles 5 and 6 of the Law. Therefore, a meticulous case-by-case evaluation must be made, and personal data shall be processed through cookies without obtaining explicit consent if other conditions are also satisfied.

In the Guidelines, clarifying explanations are also made on the explicit consent and information notice in cases where explicit consent is required. Accordingly, in obtaining explicit consent within the scope of the Guidelines, a cookies management panel should be displayed to the visitor upon visiting the website for the first time, providing the "accept", "reject", and "preferences" options equally in terms of colour, size and font. Visitors should be provided with the opportunity to grant/deny consent regarding the cookies, which cannot be used without explicit consent and the cookies applications

based on explicit consent should be displayed in a secure/passive manner at first. It is stated in the Guidelines that the opt-in system, namely a system where the data subject grants his/her consent for processing personal data with a conscious act, should be used in respect of the explicit consent statements to be obtained by data controllers from the data subjects. Also, to prevent consent fatigue, asking for explicit consent at every visit of the data subject should be avoided, and it is recommended to limit the frequency of reminding the consent preferences to the person who has rejected the use of the cookies once, periodically in proportion to the lifetime of the relevant cookies. Also, systems called "cookie walls" that prevent access to a website, and visitors from accessing a website without accepting cookies applications, are considered against the Data Protection Law.

It should be noted that the principles outlined in the Data Protection Law with the obligation to inform shall also apply to cookies, and the visitor should be informed per the Data Protection Law about the data processing activity conducted via each cookie, independently from explicit consent of the visitor or any other condition sought for processing data.

Use case scenarios are also presented in the Guidelines to concretise the good and bad cookies applications.

In a Board decision published in 2022 regarding the unlawful processing of personal data through cookies, the Board stated that explicit consent of the data subject is required when the cookies used by the data controller operating in the e-commerce sector with the aim of advertisement, marketing and performance, the privacy notice regarding cookies policy shall be easily accessible and depict clearly which personal data will be acquired with which methods and the consent of the data subjects regarding the operation of cookies with their voluntary active movements shall be ensured. The Board imposed an administrative fine on the data controller in question due to the unlawful processing of personal data.

Authors: Begüm Yavuzdoğan Okumuş, Umut Yalçın Talay, Seda Öztürk

Planned Amendments to the Law on the Protection of Personal Data

Processing Sensitive Personal Data

Proposed amendments to the Law, which have been drafted by the Board and introduce some modifications to specific disputed provisions of the Law, have been presented for the related institutions and organisations' consideration. Articles proposed to be amended are Article 6, regulating the legal grounds for processing sensitive personal data and Article 9, regulating the transfer of personal data abroad.

Under Article 6 of the Law, explicit consent from the data subject must be obtained for processing sensitive personal data. In respect of the legal grounds for processing personal data without obtaining explicit consent, while personal data relating to health and sexual life may be processed only for the purposes outlined in the Article and by authorised persons/institutions and organisations, other sensitive personal data may be processed without seeking explicit consent of the data subject, in the cases provided for by laws.

With the proposed amendment; the data included in the sensitive personal data category may be processed when processing (i) is clearly required by laws, (ii) is related to personal data made public by the data subject himself/herself, (iii) is mandatory for protection of the life or bodily integrity of a person, who is incapable of giving consent or whose consent is not legally valid, or of another person, (iv) is made by persons or authorised institutions and organisations, which are under confidentiality obligation, for the protection of public health, for conducting preventive medicine, medical diagnosis, treatment and care services, for planning and management of healthcare services and their financing, (v) is carried out for the establishment, exercise or protection of a legal right, (vi) is necessary to carry out the obligations in the field of employment, business and social security or social services, and finally (vii) is made by political parties, foundations, associations, unions or any other non-profit organisations or bodies, relating to their members on the condition that the processing relates solely to their activities and purposes, it is made in accordance with their regulations, and that personal data is not disclosed to third parties. As you may see, in case the proposed amendments are put into practice, significant changes will be made in the systematics of the current law having a dual approach to sensitive personal data, such as data relating to health and sexual life and other sensitive personal data.

With the referred amendment, which is planned to be introduced, broader legal grounds will be provided for processing sensitive personal data. Yet, the legal grounds are still limited compared to the GDPR structure regarding the conditions sought for processing data. For this reason, it would be appropriate to say that even if the current proposal is put into practice, the Law will still need to be in harmony with the GDPR.

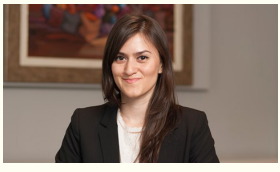
Authors: Begüm Yavuzdoğan Okumuş, Umut Yalçın Talay, Seda Öztürk

OUR TEAM

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



DİCLE DOĞAN
MANAGING ASSOCIATE

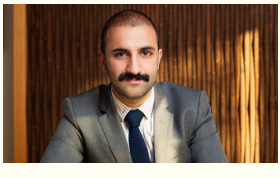
Data Protection and Privacy
Life Sciences
Intellectual Property
Trademarks and Designs

dicle.dogan@gun.av.tr

DİRENÇ BADA
MANAGING ASSOCIATE

Data Protection and Privacy
Dispute Management
Intellectual Property
Anti-Counterfeiting

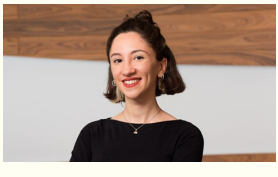
direnc.bada@gun.av.tr



YALÇIN UMUT TALAY
SENIOR ASSOCIATE

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

umut.talay@gun.av.tr



KARDELEN ÖZDEN
ASSOCIATE

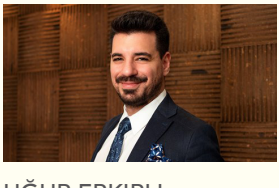
Data Protection and Privacy
Business Crimes and Anti-Corruption
Employment
Dispute Management
Corporate and M&A

kardelen.ozden@gun.av.tr

SEDA ÖZTÜRK
ASSOCIATE

Data Protection and Privacy
Corporate and M&A

seda.ozturk@gun.av.tr



UĞUR ERKIRLI
ASSOCIATE

Data Protection and Privacy
Corporate and M&A

ugur.erkirli@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.

The information and opinions provided in this content do not and are not intended to constitute legal consultancy or legal advice. This content does not constitute legal or advisory service proposal. All works and other intellectual products subject to intellectual property rights contained in this content belong to Gün + Partners and they are protected under Law No. 5846 Intellectual and Artistic Works as well as Industrial Property Code No. 6769. Unauthorized use of the content, without proper credit, would be subject to legal and/criminal sanctions as per Law No. 5846 Intellectual and Artistic Works and Industrial Property Code No. 6769.

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