GÜN + PARTNERS
AVUKATLIK BÜROSU

DATA PROTECTION AND PRIVACY LAW IN TÜRKİYE KEY DEVELOPMENTS AND PREDICTIONS

2025

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.

Introduction

In this year's report, we focus on the latest developments in the field of personal data protection, recent decisions, and published guidelines, as well as the fundamental regulations and principles of personal data protection law. Additionally, we analyse key developments in Turkiye, current significant issues in this area, and expectations, evaluations, and trends for the future.

The year 2024 has once again been marked by significant developments in personal data protection. We have witnessed the long-anticipated amendments to the Law on the Protection of Personal Data No. 6698 ("Law") coming into effect, secondary legislation efforts, and the Personal Data Protection Authority's ("Authority") guidance and publications aimed at providing direction to data controllers. Additionally, efforts were made to enhance awareness and effectiveness in personal data protection, ensure the effective implementation of the Law, and establish the proper relationship between the Law and other legal fields it intersects with, particularly competition law.

With the impact of regulations in the EU resonating in our country, discussions surrounding artificial intelligence (AI), although not yet at the desired level of maturity, have gained more prominence in 2024. In the new digital era that has taken hold worldwide, the steps to be taken in personal data protection and how to strike a balance between technology and privacy will continue to be key topics on the agenda in the coming years.

While we continue to witness positive developments each year in terms of compliance with the Law, the amendments introduced in 2024 made the second half of the year particularly intense for data controllers, as they focused on extensive compliance efforts, especially regarding cross-border data transfers.

Digital platforms, which play an increasingly central role in users' lives and pose privacy threats and risks due to large-scale data collection, processing, and sharing, remain a focal point for the Personal Data Protection Board ("Board"), as they do worldwide. With the growth of the digital economy, the data collection and processing activities of digital platforms have created a significant intersection between data protection and competition law. Notably, the competition investigation conducted by the Turkish Competition Authority against social network provider META is expected to have implications in the field of personal data protection as well.

The statistics in the information note published by the Board regarding its activities in 2024 indicate an increase in the number of notices, complaints, and applications compared to the previous year. While the Board continued its examinations intensively throughout 2024, only two of its decisions were publicly announced.

As a result of emerging practical needs and the objective of aligning the Law with the European Union's General Data Protection Regulation ("GDPR"), significant legislative amendments were introduced in the field of personal data protection in 2024. The amendments, which came into force

on June 1, 2024, marked the beginning of a new era in personal data protection, with compliance required by September 1, 2024. Within this framework, the "Regulation on the Procedures and Principles for Cross-Border Transfers of Personal Data" was published on July 10, 2024. The limited timeframe for compliance has posed challenges for both data controllers and practitioners, and for many data controllers, the compliance process is still ongoing.

In 2024, the Board continued to publish various guidelines, documents, and information notes to raise awareness in the field of data protection and provide guidance to practitioners. The Guideline on the Processing of Turkish Republic Identity Numbers outlined key considerations regarding the processing of Turkish ID numbers, which, due to their potential to grant access to other personal data, could lead to significant risks and harm if mishandled. Meanwhile, the Guideline on the Protection of Personal Data in Election Activities reminded public authorities, political parties, candidates, and voters of their obligations and rights under the Law. Additionally, the Authority published several informative materials aimed at practitioners, including the Deepfake Information Note, the Information Note on the Legal Basis for Personal Data Processing Stipulated by Law, the Information Note on the Temporal Application of Misdemeanors under Law No. 6698, the Information Note on Chatbots (Example: ChatGPT), and the Most Common Mistakes in Complaints and Notifications Submitted to the Board. These publications provided practical insights to help ensure compliance with data protection regulations.

As part of cross-border data transfers, the Standard Contract Notification Module system was established, allowing data controllers to electronically notify the Authority of standard contractual clauses, which are one of the appropriate safeguards regulated under the Law.

In 2024, the Board imposed administrative fines totaling 552,668,000 Turkish liras, with the majority of these penalties being issued against data controllers who failed to fulfil their obligation to register with the data controllers' registry and submit the required notifications despite being subject to this requirement.

In its Public Announcement regarding the Data Controllers' Registry published in August 2024, the Authority stated that the Board had initiated ex officio investigations into data controllers who failed to fulfill their registration and notification obligations. As of August 1, 2024, the Board had imposed 503,935,000 Turkish liras in administrative fines on both domestic and foreign natural and legal person data controllers who were subject to this obligation but had not complied.

As a result of the developments regarding the cross-border data transfers a total of 1,345 standard contracts were notified to the Board in 2024 (based on the Authority's records for the June–December period). These figures indicate that compliance efforts are still ongoing among data controllers.

Our report, which examines developments in the field of personal data protection and privacy under Turkish law, specifically addresses the following key topics.

Table of Content

Protection of Personal Data In Turkiye – General Approach

The primary regulation on the protection of personal data in Turkiye is the Personal Data Protection Law No. 6698 ("Law"), which came into force in 2016. Based on the European Council Data Protection Directive 95/46/EC, the Law has been influenced by the provisions of the European Union General Data Protection Regulation ("GDPR") and its implementation is shaped by both the GDPR and the decisions of European data protection authorities. The Law adopts similar objectives and fundamental concepts as the GDPR and includes largely comparable provisions regarding the basic principles of personal data protection. However, the Law is generally more limited, regulatory in nature, and less detailed compared to the GDPR.

Developments and trends in European data protection law are monitored by the Personal Data Protection Authority ("Authority"). Additionally, while the Personal Data Protection Board ("Board") follows global and European data protection trends through its principle decisions, it has also been officially announced that the Human Rights Action Plan and Implementation Schedule, published by the Ministry of Justice, will ensure the alignment of the Law with European standards and introduce regulations parallel to the GDPR.

The most significant step taken towards aligning the Law with GDPR standards was taken with the enactment of the Law No. 7499 on Amending the Code of Criminal Procedure and Certain Laws ("Amendment Law"), published in the Official Gazette on March 12, 2024. With the Amendment Law, important changes regarding the processing of special categories of personal data, cross-border data transfers, administrative sanctions, and appeals against administrative fines came into effect on June 1, 2024. In parallel with the Amendment Law, the Regulation on Procedures and Principles Regarding the Cross-border Transfer of Personal Data was also prepared and published in the Official

Gazette on July 10, 2024, entering into force on the same date. Since the enactment of the Law, the processing of special categories of personal data and cross-border data transfers have been ongoing challenges in practice, often creating bottlenecks in implementation. However, the recent amendments have provided partial solutions to these issues, contributing to Turkiye's efforts to align its data protection framework with European standards. The innovations introduced by the Amendment Law are examined below in more detail.

However, in terms of artificial intelligence (AI) regulations, it is not yet possible to say that there has been a concrete development or initiative. Currently, AI remains a subject that falls within the scope of the Law only under a single article (Article 11).

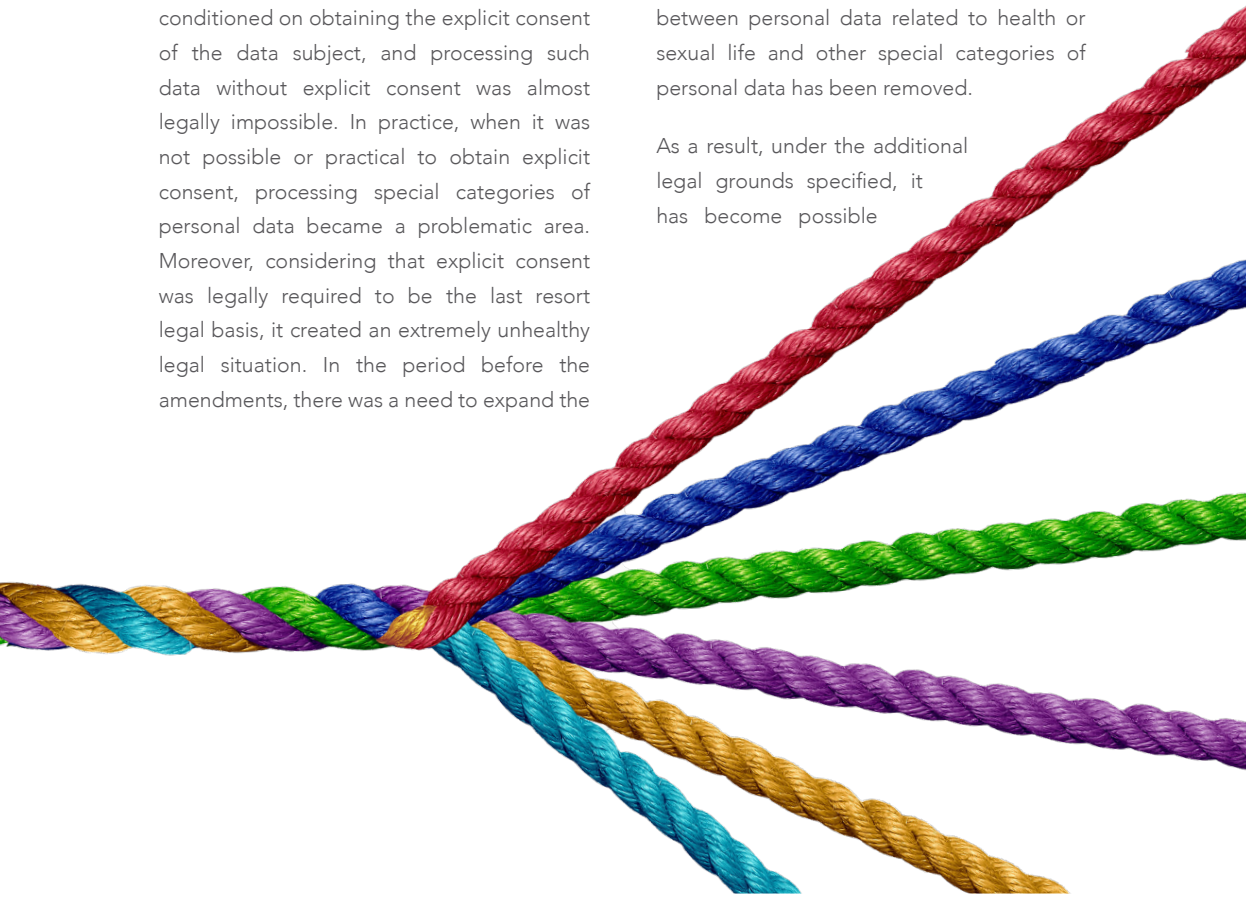
Processing of Special Categories of Personal Data

In the Law, special categories of personal data are defined in a limited manner as data related to a person's race, ethnic origin, political opinions, philosophical beliefs, religion, sect, or other beliefs, attire, membership in associations, foundations, or trade unions, health, sexual life, criminal convictions, security measures, as well as biometric and genetic data.

Before the enactment of the Amendment Law, the processing of special categories of personal data under the Law was primarily conditioned on obtaining the explicit consent of the data subject, and processing such data without explicit consent was almost legally impossible. In practice, when it was not possible or practical to obtain explicit consent, processing special categories of personal data became a problematic area. Moreover, considering that explicit consent was legally required to be the last resort legal basis, it created an extremely unhealthy legal situation. In the period before the amendments, there was a need to expand the restrictive conditions for processing special categories of personal data, as well as to address the distinction between personal data related to health or sexual life and other special categories of personal data, which was a subject of discussion in practice.

With the enactment of the Amendment Law, which aims to address the bottleneck experienced in practice and align with European and GDPR standards, the conditions for processing special categories of personal data have been expanded, and the distinction between personal data related to health or sexual life and other special categories of personal data has been removed.

As a result, under the additional legal grounds specified, it has become possible



to process all special categories of personal data without requiring the explicit consent of the data subjects.

Accordingly, all special categories of personal data (including health data and personal data related to sexual life) may only be processed if one of the following conditions is met:

i. The explicit consent of the data subject is obtained,
ii. It is expressly stipulated by laws,
iii. It is necessary for the protection of the life or physical integrity of the data subject or another person who is unable to give consent due to physical impossibility, or whose consent is not legally valid,
iv. It is relevant to personal data publicized by data subject and is in accordance with the intention of data subject of making it public,
v. It is necessary for the establishment, exercise, or protection of a right,
vi. when processing is compulsory by persons under the secrecy obligation or competent authorities or institutions for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning, management, and financing of health services,
vii. It is necessary for fulfilment of legal obligations relating to employment, occupational health and safety, social security, social services, and social benefits,
viii. where foundations, associations, and other non-profit organizations or formations established for political, philosophical, religious, or trade union purposes, provided that it is in accordance with the relevant legislation to which these organizations are subject and aligned with their stated purposes, processing is limited to their field of activity, and data is not disclosed to third parties; processing pertains to their current or former members, affiliates or individuals who are in regular contact with these organizations and formations

In the period before the amendment, data controllers processing special categories of personal data were often required to rely on explicit consent as the legal basis for most processing activities. With the amendment, however, it has become possible for data controllers to base their processing activities on different legal grounds in most cases. Legal grounds such as clear stipulation in laws, the necessity of data processing for the establishment, exercise, or protection of a right, and the necessity of fulfilling legal obligations in the areas of employment, business and social security, or social services are emerging as innovations that can help data controllers overcome the challenges they faced in practice.

In the context of employee-employer

relationships, the need to process employees' special categories of personal data due to necessity was, prior to the legislative change, only possible with explicit consent. This created operational challenges and raised debates about the validity of consent in a relationship where the employee is dependent on the employer and whether the consent could truly be given freely. With the amendment, these issues have been resolved. As a result, employers who collect and process employees' health data in the context of occupational health and safety obligations can now rely on the legal ground of "the necessity for fulfilling legal obligations in the areas of employment, occupational health and safety, social security, social services, and social assistance", and will no longer need to obtain explicit consent.

Therefore, it is crucial for data controllers to update their existing compliance practices to align with the new framework for processing special categories of personal data. In particular, they should revise their data processing policies, privacy notices, and explicit consent practices to reflect the latest legal requirements. Additionally, they must carefully assess the newly defined legal bases on a case-by-case basis for each processing activity.

Cross-Border Transfer of Personal Data

Prior to the Amendment Law, personal data could mostly be transferred abroad with the explicit consent of the data subject, as the other legal grounds specified in the legislation were either not available or not applicable. Since the Law's enactment in 2016, the fact that the Board had not yet established a list of countries providing adequate protection had significantly limited and complicated the practice of cross-border data transfer. This situation made obtaining explicit consent the only method (practically) applicable for transferring personal data abroad.

Important steps have been taken regarding this issue, which also negatively affects commercial relationships, and these steps will come into effect on June 1, 2024, with the Amendment Law. In this context, the Amendment Law introduces a three-stage assessment system for cross-border data transfer. Under the new provisions, personal data can be transferred abroad if one of the legal processing grounds specified in the Law is present and if the Board issues an adequacy decision. In cases where no adequacy decision is available, the data can still be transferred abroad if the parties involved provide one of the appropriate safeguards listed in the Law.
With the amendment, the new system for cross-border data transfer is structured as follows:

(i)Transfer of personal data abroad in the presence of an Adequacy Decision

If one of the legal grounds specified in Articles 5 and 6 of the Law exists, and if an adequacy decision is in place for the country, sector within

the country, or international organization to which the data will be transferred, personal data can be transferred abroad, including subsequent transfers. The Board will make a decision on the adequacy based primarily on the principle of reciprocity, along with other criteria. The adequacy decision will also be subject to periodic review.

It is foreseen that the Board can issue adequacy decisions not only for countries but also for international organizations or sectors within a country, and that cross-border data transfer can occur in accordance with these decisions.

(ii)In the absence of an Adequacy Decision, the transfer of personal data abroad with the provision of one of the Appropriate Safeguards

In the absence of an adequacy decision by the Board, personal data may be transferred abroad provided that one of the appropriate safeguards listed below is fulfilled and a legal ground set out in the Law is also available:

a. The existence of an agreement, which is not an international treaty, between public institutions and organizations abroad or international organizations and public institutions or professional organizations with the status of public institutions in Turkiye, and the Board's approval for the transfer.

b. Existence of binding corporate rules approved by the Board containing provisions on the protection of personal data, which the companies within the group of undertakings engaged in joint economic activities are obliged to comply with.

    i. Data controllers that are part of a corporate group can prepare binding corporate rules in accordance with the guidelines published for intra-group data transfers and submit them for approval by the Board. After these binding corporate rules are approved by the Board, cross-border data transfers can take place between the member companies of the corporate group. Although the preparation and approval processes are expected to take time, this is shaping up as a permanent solution for intra-group data transfers.

c. The existence of a standard contract published by the Board, which includes aspects such as data categories, purposes of data transfer, recipients and recipient groups, technical and administrative measures taken by the data recipient, and additional safeguards for sensitive personal data.

    i. Standard contracts, considered one of the most significant changes introduced by the Amendment Law, resemble the Standard Contractual Clauses (SCCs) under the GDPR framework.

    ii. However, the implementation of

standard contracts under the Law differs significantly from the Standard Contractual Clauses (SCCs) under the GDPR. The Board has mandated that standard contract texts must be signed without any modifications, except in explicitly permitted cases. Additionally, signed contracts must be submitted to the Authority within 5 business days from the signing date, along with documents verifying the signatories' authorization.

iii. Moreover, the published standard contracts require extensive preparation by both the data recipient and the data transferring party and necessitate the provision of information on the following matters:

i. The activities of both the data transferring party and the data recipient regarding the transferred personal data,
ii. The data subject groups whose personal data is being transferred,
iii. The categories of transferred personal data and, if applicable, the categories of transferred special category personal data,
iv. The legal basis for the transfer,
v. The frequency of the transfer,
vi. The nature of the data processing activity,
vii. The purposes of data transfer and subsequent processing activities,
viii. The retention period of personal data,
ix. The recipients or recipient groups,
x. The data controller's registration details in the Data Controllers' Registry Information System (VERBİS),
xi. In cases of transfer to data processors or sub-processors, the subject, nature, and duration of the processing activity,
xii. The technical and administrative measures implemented, and, if special categories of personal data are transferred, the additional technical and administrative measures taken specifically for such transfers,
xiii. If applicable, the list of sub-processors.

d. The existence of a written undertaking containing provisions to ensure adequate protection and authorization of the transfer by the Board.

i. Finally, in cases where no adequacy decision exists or data controllers transferring data cannot provide any of the appropriate safeguards, certain exceptions are provided only for incidental transfers. In other words, these exceptions apply to irregular, one-time, or occasional transfers that are not part of routine business operations. However, since these

exceptions are limited to specific cases, data controllers are advised not to rely on them for regular and systematic cross-border data transfers. Instead, they should ensure that their data transfer processes comply with the other appropriate safeguards specified in the Law. The exceptions include:

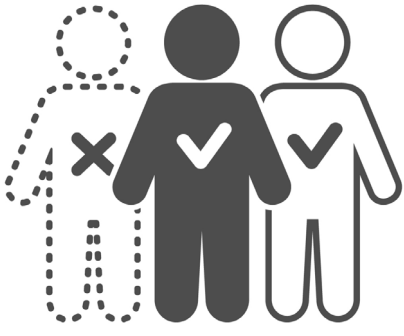
- Provided that data subjects are informed about potential risks, they may give explicit consent to the transfer,
- The transfer is necessary for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures taken at the request of the data subject,
- The transfer is necessary for the conclusion or performance of a contract made in the interest of the data subject between the data controller and another natural or legal person,
- The transfer is necessary for overriding public interest,
- The transfer is necessary for the establishment, exercise, or defense of a legal right,
- The transfer is necessary for the protection of the life or physical integrity of the data subject or another person in cases where the data subject is unable to express consent due to actual impossibility or when their consent is not legally valid,
- The transfer is carried out from a public register or a register accessible to persons with a legitimate interest, provided that the conditions required by the relevant legislation for access to the register are met and the request comes from a person with a legitimate interest.

It should be noted that, with the Amendment Law, data transfers based on the legal ground of explicit consent have been regulated in a manner that is only accepted in exceptional cases. Since most cross-border data transfers in practice were previously based on explicit consent, a transition period has been introduced by adding a temporary article to the Law under the Amendment Law. Accordingly, until September 1, 2024, it will still be possible to transfer personal data abroad based on explicit consent. In this context, after September 1, 2024, data controllers must ensure that they comply with one of the appropriate safeguards stipulated in the Law for regular cross-border data transfers, considering that no adequacy decision has been issued yet. Given that the transition period provided by the temporary provision has also ended, data controllers who have not yet aligned their cross-border data transfer processes must immediately identify the scope of their cross-border data transfers in detail, determine which companies they are transferring data to, and complete the necessary work as soon as possible to ensure compliance with one of the appropriate safeguards provided in the Law..

Finally, with the Amendment Law, a new administrative fine has been added to the Law. As mentioned above, if data controllers and data processors fail to comply with the obligation to notify the Personal Data Protection Authority within 5 business days about the standard contracts they sign for international data transfers, they will face administrative fines ranging from 71,965 Turkish Liras to 1,439,300 Turkish Liras for 2025, with the reassessed rate. Additionally, if it is determined that an appropriate safeguard has not been provided in the international data transfer processes by data controllers by September 1, 2024, there is a risk of an administrative fine ranging from 204,285 Turkish Liras to 13,620,402 Turkish Liras for 2025.

Data Controllers' Registry (VERBIS)

Pursuant to Article 16 of the Law, data controllers who meet certain criteria are obliged to register with the Data Controllers' Registry ("VERBIS"). The procedures and principles regarding the VERBIS system, which is open to the public, are determined by the "Regulation on the Data Controllers Registry" dated December 30, 2017 ("VERBIS Regulation").



With the Board's decisions dated 2018, various professional groups, associations, foundations and political parties were exempted from VERBIS registration obligation and minimum criteria based on the number of employees and balance sheet were introduced for data controllers residing in Turkiye in determining the registration obligation and those who will be exempted from the registration obligation.

Regarding the aforementioned minimum criteria, with the decision published in 2023, the Board updated the annual financial balance sheet total amount in the criterion of having an annual financial balance sheet total of more than 25 million Turkish Liras, which is one of the criteria used in determining the data controllers exempted from the VERBIS registration obligation, and increased the annual financial balance sheet total amount to 100 million Turkish Liras. Among the natural or legal person data controllers whose annual number of employees is less than 50 and whose annual financial balance sheet total is less than 100 million Turkish Liras, data controllers whose main activity is not processing special categories of personal data are exempted from VERBIS registration. It should also be noted that for data controllers resident in Turkiye, crossing only one of the limits regarding the number of employees or the annual financial statement total is sufficient for the VERBIS registration obligation to be triggered, and for data controllers residing abroad, these criteria are not applied in the assessment of the obligation.

Accordingly, the range of administrative fines to be imposed in case of violation of the VERBIS registration obligation for 2025 will be between 272,380 Turkish Liras and 13,620,402 Turkish Liras. The Board uses certain algorithms to determine the amount of the fine, and accordingly, the higher the total assets in the financial balance sheet within the specified fine range is, closer the fine amount gets to the upper limit.

The Board actively monitors data controllers residing in Turkiye in light of their notifications to the Social Security Institution and tax authorities and may impose administrative

fines on data controllers who exceed the thresholds without warning if they fail to fulfil their registration obligations. The Board also investigates data controllers residing abroad who process data of Turkish residents and may impose fines on these data controllers as well. Therefore, in order to minimize the risks of fines, it is recommended to regularly check and monitor the registration obligation.

At this point, it should be noted that the Law also applies to data controllers (resident in Turkiye or providing goods and services to Turkiye) who target data subjects in Turkiye, regardless of their nationality even if they do not reside in Turkiye. Thus, the obligation to register with VERBIS arises in the event that data controllers residing abroad engage in personal data processing activities in Turkiye, either directly or through their branches or process personal data transferred to them for their own purposes.

Therefore, non-resident legal entities that are parents of a resident data controller will be obliged to register with VERBIS if they process the personal data transferred to them as a data controller for their own purposes. The distinction to be noted at this point is that the activities of the legal entity must actually target data subjects in Turkiye and process the relevant personal data as a data controller for its own purposes. The mere fact that personal data is kept in the data registry system of a legal entity residing abroad will not give rise to a VERBIS obligation.

Data controllers residing in Turkiye who have not yet registered with VERBIS must assess their annual employee numbers and annual financial statements each year to determine whether they have a VERBIS registration obligation. Particularly in light of recent developments in international data transfers, data controllers who have signed and reported standard contracts related to cross-border transfers to the Board but have not fulfilled their VERBIS obligations will attract attention. Therefore, institutions acting as data controllers and located abroad should check their VERBIS obligations and ensure that their VERBIS registration is completed no later than the submission of the relevant standard contracts to the Board.

Finally, it is worth noting that, pursuant to the VERBIS Regulation, foreign-based data controllers who are obliged to register with VERBIS must appoint a data controller representative to act as a point of contact in their relations with the Board, the Authority and data subjects. The data controller representative may be a legal entity resident in Turkiye or a natural person who is a citizen of the Republic of Turkiye. The appointment of a representative must be made by a notarized and apostilled (or otherwise certified) decision of the data controller. If a legal entity is appointed as a representative, a natural person must also be appointed by the foreign data controller to act as a contact person.

Protection of Personal Data In the Field of Artificial Intelligence

With the rapid expansion of the use of artificial intelligence (AI) and its integration into all areas of life, it has become essential to establish a legal framework that regulates the safe and ethical development, distribution and use of AI systems, considering the complexity and unique characteristics of this technology.

In addition to promoting the safe, transparent, and human rights-respecting development of AI technologies, and aiming to protect the safety, rights, and freedoms of users and society, the European Union Artificial Intelligence Act ("AI Act"), which came into force on August 1, 2024, to ensure the ethical development of AI and the protection of personal data. As a pioneering regulation, it is considered that the AI Act will guide many countries in determining their national policies and strategies and in legislative efforts concerning AI and related issues.

Unlike the regulations made in the European Union, there is currently no specific regulation on artificial intelligence in Turkiye. However, with the widespread use of artificial intelligence applications in Turkiye, the creation of legal and regulatory frameworks in this area has become one of the key issues on the agenda.

2024 was a year in which important steps were taken in the development and implementation of artificial intelligence technology in Turkiye. Within the scope of the "National Artificial Intelligence Strategy" prepared for the years 2021-2025, Turkiye has also created an action plan for 2024-2025, outlining a roadmap for the development and use of this technology. The action plan includes actions such as preparing a report on the legal assessment of artificial intelligence applications and monitoring their compliance with laws, but a specific legal regulation for artificial intelligence has not yet been foreseen. On the other hand, independent of the action plan, some efforts have been made to regulate artificial intelligence legally, and the first draft law on this topic was presented to parliament in 2024. Although this draft law is considered not to provide a sufficient framework yet, it is

expected that Turkiye will adopt an approach similar to the European Union's regulations on artificial intelligence.

The Personal Data Protection Authority has not remained indifferent to the developments in the field of artificial intelligence. In its publication titled "Recommendations for the Protection of Personal Data in the Field of Artificial Intelligence," it shared its suggestions for developers, manufacturers, service providers, and decision-makers involved in artificial intelligence activities regarding the protection of personal data under the Law. It is worth noting that the recommendation published by the Board includes main elements of Article 22 of the GDPR which once again shows us the fact that the Board has its guidance from the GDPR and although not yet enacted officially, the principals under Article 22 of the GDPR are already taken into account by the Board. According to the recommendations, AI applications should be managed with a human-centered approach. Algorithms that ensure accountability in compliance with data protection laws must be adopted from the design phase of products and services and throughout their entire lifecycle. Risk assessments must be conducted with the participation of individuals and groups likely to be affected by the applications.Products and services must be designed to ensure that individuals are not subjected to decisions affecting them solely based on automated processing without considering their exclusive views.

If the same outcome can be achieved without processing personal data in the development of artificial intelligence technologies, the data must be processed in an anonymised form.

In artificial intelligence initiatives, all systems must be developed in accordance with the principle of data protection from the design phase onwards.

Human intervention must be established in decision-making processes, and individuals' freedom to distrust the outcomes of AI-generated recommendations must be preserved.

The quality, nature, source, and quantity of personal data used should be assessed to ensure minimal data usage, and the accuracy of the developed model must be monitored. If high risks are anticipated in terms of personal data protection in AI projects, a privacy impact assessment should be carried out, and the lawfulness of data processing activities must be evaluated within this framework.

To raise awareness of personal data protection, training and information initiatives on data privacy must be encouraged.

The processes of collecting, analyzing, and using personal data by artificial intelligence systems raise significant questions regarding individuals' privacy rights and compliance with data protection regulations. The Law mandates principles such as transparency, data minimization, legality, and accountability in the development and use of artificial intelligence. Managing AI systems in a legally sustainable manner is crucial from a legal perspective and the Law definitely needs a revision and detailed rules on this.

Cookies

Cookies play a crucial role in personalizing and improving the user experience in the digital world. Although the use of cookies contributes greatly to personalizing the internet experience and remembering users' online preferences, this process has also raised various privacy and data protection concerns. One of the biggest concerns regarding the processing of personal data through cookies is that users are often unaware of this process or that sufficient transparency is not provided regarding the use of cookies. Since cookie policies and privacy statements are often not presented in a manner that is easily accessible and understandable to users, this situation prevents users from knowing how to protect their online privacy. As a result, they lack sufficient control over their data, which makes it difficult to manage it and restrict their online tracking.

As a result of the privacy and data protection concerns that are frequently discussed among practitioners regarding cookies, in recent years, many countries, including Turkiye, have seen data protection authorities establish rules and principles regarding the processing of personal data through cookies, publish guidelines, and issue decisions imposing penalties on data controllers.

The Board prepared a document titled the "Guidelines on Cookies Applications" ("Guidelines") with the aim of providing recommendations and guidance to data controllers processing personal data through cookies. This Guidelines was published on the Board's website in June 2022. The Guidelines generally addresses cookies and their types, and it also classifies cookie types according to their duration, purposes of use, and parties involved. In the Guidelines, the relationship between Law No. 5809 on Electronic Communications ("ECL") and the Personal Data Protection Law is also examined. It explains that if a cookie is used solely for providing communication via an electronic communications network and if the data controller holds the status of an operator within the scope of the ECL, data processing can take place without obtaining explicit consent. The Guidelines states that except for the limited cases mentioned above, where the ECL applies to cookie practices, the provisions of the Personal Data Protection Law will apply, and the principles and legal bases for data processing set forth in the Law

must be observed even when personal data is processed through cookies.

The Guidelines also include detailed explanations regarding explicit consent and disclosure for cases where explicit consent is required. Accordingly, when obtaining explicit consent under the Guidelines, a cookie management panel should be displayed to the visitor as soon as they enter the site, offering "accept," "reject," and "preferences" buttons in equal color, size, and font. The visitor should have the opportunity to approve or disapprove cookies that cannot be used without explicit consent via the preferences button, and cookie applications based on explicit consent should initially be in a closed/passive state. The Guidelines states that the explicit consent declarations obtained from individuals by data controllers must follow an opt-in system, meaning that individuals must give prior approval for the processing of their personal data through a conscious action. Additionally, to prevent consent fatigue, it is emphasized that explicit consent should not be requested every time the individual visits the site. For visitors who have once rejected cookies requiring explicit consent, reminders should only be made periodically in proportion to the lifespan of the relevant cookie. Furthermore, systems known as "cookie walls," which block access to a website and prevent visitors from using the site unless they consent to cookie applications, are not considered compliant with the Law.

It should be noted that the principles established by the Law regarding the obligation to inform also apply to cookies in the same manner. Regardless of whether data processing through cookies is based on the visitor's explicit consent or another legal basis, visitors must be informed in compliance with the Law for each data processing activity carried out via cookies.

The Guidelines, sheds light on all aspects of cookie usage, including legal grounds, cases requiring consent, legal conditions for consent, and information processes, also highlights key points that data controllers should pay attention to. Additionally, the subject has been made more concrete with clear and understandable examples.

It is crucial for data controllers to review the compliance of their current cookie practices with the Guide published by the Authority and to ensure that their personal data processing activities through cookies are in line with the law. Indeed, when examining cookie practices, it is observed that some do not provide users with a "reject" option, some do not offer the rejection option as easily as the acceptance option, and some still use the opt-out system. In addition to incorrect implementations, even in cases where cookie practices are designed in accordance with the Guide, it should not be forgotten that ensuring sufficient transparency in cookie usage terms, as well as making access to informative texts difficult through hyperlinks, can undermine the validity of explicit consent.

Data Breach and Its Consequences

The Law requires data controllers to notify the Board and the data subject as soon as possible after becoming aware of the data breach. In its decision dated January 24, 2019 and numbered 2019/19 ("Decision"), the Board clarified the rules and procedures to be followed in data breach cases.

The Board adopted the approach of the GDPR in terms of the timing of breach notifications and explained that the phrase "as soon as possible" in the Law must be interpreted as within 72 hours after the data breach is detected.

The Law also requires data controllers to notify data subjects as soon as they identify data subjects affected by the data breach, regardless of whether the risk is low or not. In the aforementioned Decision, the Board did not stipulate a specific period of time regarding the duration of the notification to be made after the identification of the data subjects affected by the data breach, and stated that the notification should be made as soon as reasonably possible. Although reasonable time is a matter that should be evaluated in each concrete case, it would be appropriate to notify the relevant persons immediately after the notification of the data breach to the Board.

The Board's decision requires data controllers to draw a roadmap in advance and clarify internal reporting mechanisms and procedures to be followed in order to be prepared for data breaches. Data controllers are obliged to keep records of data breaches and measures taken.

The obligation to report a data breach also applies to data controllers residing abroad. In the event that data controllers abroad experience a data breach and the data breach in question affects data subjects residing in Turkiye and goods/services used by data subjects in Turkiye, data controllers abroad are likewise obliged to follow the data breach notification procedures announced by the Board. The critical issue for data controllers

abroad is that even if the data breach occurs abroad, the Board must be notified if the data subjects affected by the data breach are located in Turkiye. In this sense, the scope of application of the Law has been expanded in terms of data breach notifications.

The Board has also published a "Personal Data Breach Notification Form" for data controllers to fill out when notifying the Board. When examining the data breach notifications published on the Institution's website, it is observed that while most of the notifications have been made by private companies, breaches have also been reported by institutions such as hospitals and universities. On the other hand, the categories of individuals affected by the breaches predominantly consist of the relevant data controllers' employees, patients, subscribers, customers, students, clinical research participants, and business partners. Regarding the affected data categories, it is noted that they mainly include identity, education, health, association membership, transaction and physical space security, criminal convictions and security measures, race and ethnic origin, accounting and financial information, as well as genetic and biometric data. These data breach notifications have been made from both domestic and international sources.

Additionally, a significant portion of the published data breaches appear to have resulted from cyber-attacks targeting data controllers in the plastics industry and related sectors. Another major portion consists of data breaches reported by data controllers receiving services from a service provider that was subjected to an attack involving the infiltration of its management panel. In conclusion, when looking at the year 2024, it is observed that data breach notifications have been made by data controllers from a wide range of industries and sectors.

When examining the 2024 data breach statistics, a total of 81 data breach notifications were submitted to the Board, and 63 of these notifications were publicly announced. A review of the data breach notifications published on the Authority's website reveals that data breaches generally occur as a result of ransomware attacks, cyberattacks, unauthorized access to user accounts, the compromise of an internal user's credentials, data leaks, data deletion, server lockouts, infiltration of the admin panel, public online exposure of data, and phishing attacks.

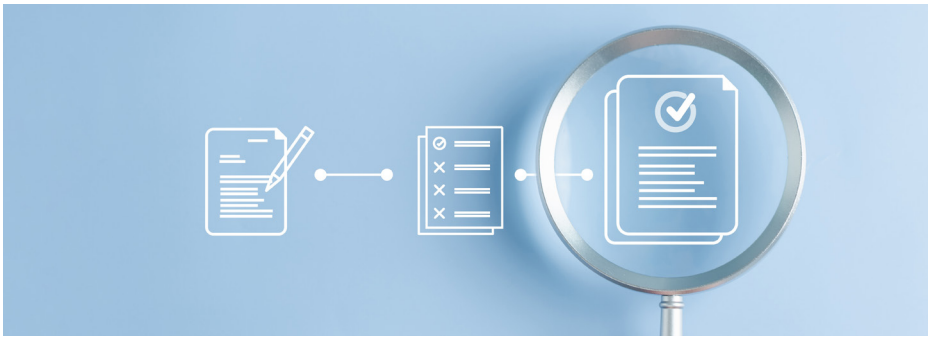
A data breach, in terms of its consequences, poses a risk of administrative fines for the data controller and must also be carefully considered due to potential criminal liability under the Turkish Criminal Law. As is known, the law includes provisions for both administrative fines and criminal liability. Regarding criminal liability, the law refers to the relevant provisions of the Turkish Criminal Law, which set out sanctions for the unlawful recording, disclosure, or acquisition of personal data.

In addition to criminal sanctions, the law also includes provisions detailing the administrative fines applicable in the event of a violation. Failure to fulfill data security obligations, data breaches, and failure to report a breach to the Board in a timely manner may result in administrative fines ranging from 68,083 Turkish Lira to 13,620,402 Turkish Liras (updated for 2025) for data controllers.

In the cases reviewed and announced by the Board regarding data breach notifications, it is observed that the Board tends to impose penalties, in contrast to the more constructive approach adopted by European data protection authorities. However, it should also be noted that the Board has issued decisions where no administrative fines were applied, considering factors such as the number of individuals affected by the breach, whether the breach had a negative impact on the data subject, whether the data controller could intervene, whether the breached data was deleted, whether the data controller reported the breach within the required timeframe, and whether reasonable administrative and technical measures were taken.

Proper and timely handling of data breach processes is critically important for data controllers. In addition to the principles and procedures established and implemented by data controllers regarding the processing, deletion, destruction, and disposal of personal data, it is essential to clearly define the procedures to be followed in the event of a data breach. Establishing a data breach response plan as part of compliance processes will contribute positively to minimizing the risks associated with a potential data breach by enabling a swift and effective response.

Judicial Review of Board Decisions



Pursuant to the Law, the Board has the authority to impose administrative sanctions. It has been regulated that the Board may impose administrative fines for non-compliance with the obligation of disclosure, obligations related to data security, failure to comply with the decisions issued by the Board, violations of the obligation to register and notify the Data Controllers' Registry, or non-compliance with the notification obligation regarding standard contracts. In addition to imposing administrative fines, the Board may also decide to order the data controller to eliminate the breach and to suspend data processing and transfer as an administrative action.

Within the systematics of the Law, administrative fines to be imposed by the Board are regulated under the title "Misdemeanors". Accordingly, within the framework of the revaluation rate regulated under Article 298 (repeated) of Tax Procedure Law No. 213, the administrative fines specified in the relevant articles of the Law will be applied as follows in 2025:

Administrative Fines under the Law for 2025		
Legal Basis	**Breach Type**	**Current Administrative Fine**
Article 18/1/a of the Law	Failure to fulfil the disclosure obligation	TRY 68,083 – 1,362,02
Article 18/1/b of the Law	Failure to fulfil the data security obligations	TRY 204,285 – TRY13,620,402
Article 18/1/c of the Law	Failure to comply with the Board's decisions	TRY 340,476 – TRY 13,620,402
Article 18/1/ç of the Law	Failure to fulfil the obligations of register and notify the Data Controllers Registry	TRY 272,380 – TRY 13,620,402
Article 18/1/d of the Law	Failure to notify the Authority of Standard Contracts within 5 business days	TRY 71,965 – TRY 1,439,300

On the other hand, prior to the amendments, the Law did not provide any avenues for challenging administrative fines and sanctions imposed by the Board, and this issue was not regulated within the Law. In practice, since violations that result in administrative fines were classified as "misdemeanors," the legal avenues for appealing these sanctions were based on the Misdemeanor Law No. 5326. As a result, lawsuits against these administrative fines were typically brought before Criminal

Courts of Peace, which were considered to have jurisdiction in such cases. In response to this situation, practitioners have long criticized that, given the highly technical and specialized nature of personal data protection, the Criminal Courts of Peace, which are primarily focused on criminal law, are not the appropriate authority for the judicial review of decisions made by the Board. It has been observed that decisions made by the Criminal Courts of Peace are often superficial and lack legal justification, and this has led to the view that such decisions cause rights violations for individuals. On the other hand, the fact that appeals against decisions made by Criminal Courts of Peace are reviewed by another criminal peace court has resulted in these decisions becoming final without undergoing review by a higher court, thus hindering the creation of case law in the field of personal data protection law.

When the judicial review process conducted by the Criminal Courts of Peace, which are first-instance courts, is completed with the finalization of the decision through a simplified trial procedure, the only available avenue for higher court review is to appeal directly to the Constitutional Court. Indeed, in a recent decision, the Constitutional Court determined that the judicial process concerning the administrative fine imposed by the Board on a data controller for violating its obligations to ensure data security led to a violation of the right to property. In its ruling, the Constitutional Court emphasized that administrative fines constitute an interference with the right to property. Therefore, it concluded that, when interfering with property rights, the general principles governing the limitation of fundamental rights and freedoms under Article 13 of the Constitution must be taken into account, and the interference must comply with the principle of proportionality. Under the principle of proportionality, it was stated that interventions should be proportionate and that it is of great importance for a court to effectively examine claims of unlawfulness in terms of the proportionality of the intervention. Ultimately, the Constitutional Court ruled that the judicial review carried out by the Criminal Courts of Peace did not include any assessment within the framework of the objections made by the appealing party. Therefore, it was found that the safeguards for the protection of the right to property under the right to a fair trial were not fulfilled, leading to a violation of the right to property.

As highlighted by the Constitutional Court's decision, it is of great importance for a court to effectively examine claims of unlawfulness in ensuring the proportionality of interventions made to fundamental rights and freedoms.

The findings regarding the difficulties in the judicial process against the administrative fines imposed by the Board, the criticisms raised, and the Constitutional Court's decision have demonstrated that the Criminal Courts of Peace are not the appropriate authority

for judicial review in the field of personal data protection. With the publication of the Human Rights Action Plan by the Ministry of Justice, it was announced that the Law would be aligned with European Union standards, and individuals would have the option to appeal the Board's administrative fines to administrative courts instead of Criminal Courts of Peace.

With the Amendment Law, a clear regulation has been introduced as a solution to these issues, allowing administrative lawsuits to be filed against the Board's administrative fines in administrative courts. In this way, it has been explicitly regulated that the administrative fines imposed by the Board, being administrative acts, will be subject to administrative judicial review, thereby eliminating uncertainties in practice and establishing a procedure that will enable more effective oversight of the Board's decisions. With this amendment, it is expected that the legal certainty issues experienced in the pre-amendment period will decrease and that jurisprudence providing guidance for practice will increase.

With the Amendment Law coming into force on June 1, 2024, a transitional provision has been introduced, stipulating that applications already pending before the Criminal Courts of Peace before the effective date will continue to be handled by these courts.

According to this transitional provision, cases that are still ongoing before the criminal judgeships of peace as of June 1, 2024, will be finalised by these courts. However, lawsuits filed after June 1, 2024, will be heard before administrative courts.

Although the temporal application of the Law has been determined through the amendments and the added transitional provision, the other transitional provisions—particularly those concerning the cross-border transfer of personal data, which allow the continuation of the previous practice until 01.09.2024—have raised questions regarding the temporal application of the Law in practice.

In order to eliminate these uncertainties, the Authority published an informational note on 19.12.2024 to serve as a guide for implementation. It emphasized that the provisions regarding temporal application in the Turkish Criminal Law No. 5237 would be taken into account.

Within this framework, the administrative sanction decision to be applied will be determined based on the principles of the Turkish Criminal Law, considering the time of the offence and the time of the complaint. Accordingly;

- In cases where the act was committed and completed before the legislative amendment:

- In cases where the act was committed and completed before the legislative amendment, regardless of when the complaint was filed, if the decision to be issued as a result of the trial is made after the Effective Date of the Amendment Law, the more favorable law will be applied.

- In cases where the act began before the legislative amendment and is still ongoing (continuous acts – ongoing violations);
  - If the act was ceased before the legislative amendment, the law that is more favorable to the offender will be applied and,
  - If the act continues and ceases after the legislative amendment, the new law enacted after the amendment will be applied.
- If the act occurred after the legislative amendment:
  - In such cases, no issue regarding the temporal application of the law will arise, and the new law will be applied.

KEY CONTACTS

BEGÜM YAVUZDOĞAN OKUMUŞ
PARTNER

begum.yavuzdogan@gun.av.tr

DİCLE DOĞAN
MANAGING ASSOCIATE

dicle.dogan@gun.av.tr

DİRENÇ BADA
MANAGING ASSOCIATE

direnc.bada@gun.av.tr

YALÇIN UMUT TALAY
MANAGING ASSOCIATE

umut.talay@gun.av.tr

SEDA TAKMAZ
SENIOR ASSOCIATE

seda.ozturk@gun.av.tr

GÜNCE GÜNEŞ CEYLAN
ASSOCIATE

gunes.ceylan@gun.av.tr

UĞUR ERKIRLI
ASSOCIATE

ugur.erkirli@gun.av.tr

Firm Overview

We are one of the oldest and largest law firms in Turkey and are considered internationally to be among the top-tier of legal services providers.

We are a full-service law firm leading the intellectual property field among others, providing dispute management, advisory, transactional, prosecution, investigation, and regulatory markets law services to domestic and multinational corporations.

We are based in Istanbul, with working and correspondent offices in Ankara, Izmir and the major commercial centres in Turkey.

We operate mainly in Turkish and English and also work fluently in German and French.

We advise a large portfolio of clients in numerous fields of activity including life sciences, insurance and reinsurance, energy, construction & real estate, logistics, technology, media and telecoms, automotive, FMCG, chemicals and the defense industries.

Our vision is to be the leader in the services we provide, sensitive to wider society, the environment, and our employees as an innovative and sustainable institution.

Our clients' success is at the heart of our own success. We closely monitor developments in the business sectors in which our clients operate and invest in accumulating industry specific knowledge to understand their changing needs. We actively participate in professional, trade and business organisations in Turkey and internationally.

We are committed to adapt to our clients' changing business needs by delivering innovative, high quality and commercially prudent legal solutions.

GÜN + PARTNERS
AVUKATLIK BÜROSU

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
Istanbul, Turkey

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

www.gun.av.tr