JANUARY 2025 Gökçe ISSUE: 134

THE FINE PRINT

Answers. Not theories.

CYBER SECURITY BILL IS AT THE NATIONAL ASSEMBLY: TURKEY'S NEW ERA IN CYBER SECURITY

- Turkish TV and Film Industry: Monopolization Allegations Spark Attention
- The Concern Entering Entrepreneurs' Agenda with "Getir": Shareholder Disputes
- Notable Developments in the World of Personal Data

Cyber Security Bill is at the National Assembly: Turkey's New Era in Cyber Security

Turkey has reached a crucial milestone in the field of cyber security: The Cyber Security Bill **(Bill)** was proposed to the Grand National Assembly of Turkey **(Assembly)** on 10 January 2025. However, it is also expected that there will be provisions that may be subject to change until publication.

Until now, there was no comprehensive framework legislation regulating the field of cyber security under Turkish legislation, such as the "Law on the Protection of Personal Data" or the "Law on the Regulation of Electronic Commerce". Now, with the Bill, a ground-breaking era will be entered in the cyber security area.

The main purpose of the Bill is to determine strategies and policies to strengthen cyber security in the Republic of Türkiye.

The Bill covers all public institutions and organizations, professional associations, real and legal persons operating in cyberspace. The activities carried out by the National Intelligence Organisation and the General Directorate of Security and the Gendarmerie General Command, which are of an intelligence nature, are excluded from the scope of the Bill.

The outstanding regulations in the Bill are as follows:

- Establishment of the Cyber Security Board and its duties and powers,
- Increasing the cyber resilience and maturity levels of public institutions and critical infrastructure organizations,
- Centralised monitoring, detection, and elimination of cyber security incidents,
- Implementation of deterrent sanctions through audit processes,
- Regulation of standardization, certification and authorization processes,
- Implementation of severe penalties for cybercrimes and incidents.

Significant definitions in the Bill are as follows:

The President refers to the Cyber Security President, and the Presidency refers to the Cyber Security Presidency. At this point, the Presidency assumes a proactive role against cyber threats. This role includes vital responsibilities such as increasing the cyber resilience of critical infrastructures, detecting, preventing and mitigating cyber attacks.

The scope of information systems is broadly defined in the Bill. Accordingly, information systems include hardware, software, systems and all other active or passive components used in the provision of all kinds of services, transactions and data provided by information and communication technologies.

Cyberspace is defined as "the environment consisting of information systems connected to the Internet or electronic networks and the networks connecting these systems." This definition makes it clear that everyone operating in the digital world will be subject to the Bill.

"SOME" is defined as Cyber Incident Response Team. The Presidency has the authority to establish, ensure and supervise the establishment of SOMEs, to carry out studies to determine and increase their maturity levels, and to measure the cyber incident response capabilities of SOMEs by organizing cyber security practices.

Although not included in the definitions section, the Bill calls for the establishment of a Cyber Security Board **(Board).** The purpose of the Board is to make decisions on policies, strategies, action plans and other regulatory actions related to cyber security and to determine the institutions and organizations that will be exempted from all or some of the decisions taken.

The main duties and responsibilities regarding cyber security of those who are covered by the Bill and who provide services, collect, process data and carry out similar activities by using information systems are as follows:

All kinds of data, information, documents, hardware, software and any other contribution requested by the Presidency within the scope of its duties and activities should be transmitted to the Presidency primarily and on time. This point is quite critical since the violation of this regulation brings imprisonment and administrative fines.

- Measures stipulated by the legislation should be taken for the purposes of national security, public order or the proper execution of public service for cyber security, and vulnerabilities or cyber incidents detected in the area where service is provided should be notified to the Presidency without delay.
- Cyber security products, systems and services to be used in public institutions and organizations and critical infrastructures should be obtained from cyber security experts and companies authorized and certified by the Presidency.
- Cyber security companies subject to certification, authorization and certification must obtain the approval of the Presidency before commencing operations.

In this context, the Presidency may inspect all kinds of acts and transactions falling within the framework of the Bill when it deems necessary in relation to its duties specified in the Bill; for this purpose, it may conduct on-site inspections or have them conducted.

The criminal sanctions within the scope of the Bill are as follows:

- Three to five years imprisonment for those who unauthorisedly access, share, or offer for sale personal or critical public service data as a result of data leaks in cyberspace,
- Those who commit a cyber-attack against the elements constituting Turkey's national power in cyberspace or who keep any data obtained as a result of this attack in cyberspace will be sentenced to imprisonment from eight to twelve years, unless the act constitutes another offense requiring a heavier penalty; those who disseminate, send elsewhere or offer for sale any data obtained as a result of this attack in cyberspace shall be sentenced to imprisonment from ten to fifteen years.
- From one million Turkish liras to ten million Turkish liras for those who fail to fulfill their duties and responsibilities to take the measures stipulated by the legislation for the purposes of national security, public order or proper execution of public service regarding cyber security, to notify the Presidency without delay of the vulnerabilities or cyber incidents they detect in the

field they provide services, and to procure cyber security products, systems and services to be used in public institutions and organizations and critical infrastructures from cyber security experts and companies authorized and certified by the Presidency,

- Those who fail to fulfill the obligations imposed on companies offering cyber security products and services will be fined an administrative fine of ten million Turkish liras to one hundred million Turkish liras.

- Those who carry out activities aimed at targeting institutions or individuals by creating a perception of data leakage in cyberspace, even though there is no data leakage, will be sentenced to imprisonment from two to five years. The relevant regulation has caused widespread resonance within public opinion. The main reason for this is that the expression "creating a perception as if a data leak had occurred" in the article is open to broad interpretation.

The sale abroad of cyber security products, systems, software, hardware and services established or developed with public support, and the merger, division, share transfer or sale transactions of the companies producing them will be subject to the approval of the Presidency.

In addition, if the Bill passes through the Assembly, companies in the field of cyber security will have to complete their certification processes within one year from the publication of the passed Bill in the Official Gazette.

Developments in the field of cyber security and the regulations to be introduced by the Bill are eagerly awaited. You can access the Bill here. *(Only avaliable in Turkish)*.

Turkish TV and Film Industry: Monopolization Allegations Spark Attention

As known, in competition law terms, monopolization means that a company establishes dominance over a particular good or service. This may be achieved through the acquisition of competitors, exclusion of competitors from the market, patenting a unique invention, or legally granting trade rights only to that company. As a matter of fact, it is a critical issue in terms of a free market economy that monopolization provides a great advantage to producers while creating disadvantageous results for consumers.

Recently, Turkish society's agenda has been dominated by the investigation launched against casting agencies.

The Competition Board **(Board),** with its announcement dated 8 January 2025, announced that the preliminary investigation conducted with the allegation that certain casting agencies and managers violated the Law on the Protection of Competition **(LPC)** has been completed. The Board decided that the information and documents obtained were serious and sufficient and initiated an investigation into 21 undertakings operating in the relevant sector.

Two main topics stand out in the complaints received by the Board: Firstly, the allegation that some casting agencies and managers acted jointly to determine commission rates and sales conditions and tried to boycott some producers and push them out of the market. Secondly, the allegations that undertakings carrying out casting director and agent activities together distort competition by giving advantages to their own actors in projects and disadvantage independent actors and agencies.

All these allegations will be assessed in terms of the prohibition of agreements, concerted practices and decisions restricting competition between undertakings and the prevention of an undertaking from abusing its dominant position within the scope of the LPC. In particular, the investigation process is expected to examine in detail the allegations that casting agencies and managers try to determine commission rates and sales conditions together.

The Board's investigation will be an important step towards ensuring transparency and fair competition in the TV series and film industry. The decisions to be taken as a result of the investigation may set a precedent for all parties in the sector.

You can reach the relevant announcement of the Competition Board here.

The Concern Entering Entrepreneurs' Agenda with "Getir": Shareholder Disputes

Getir, one of Turkey's most successful startups, has garnered international recognition with its impressive achievements. Recent investor/shareholder disputes involving Getir have created a cautious atmosphere, prompting everyone to act with potential disputes in mind.

To briefly recap, in June 2024, under an agreement, the management and majority shares of the company's operations in Turkey were transferred to a foreign investment fund. While the restructuring aimed to ensure financial stability, allegations emerged that the agreement was violated and that the founders' rights were being unfairly disregarded.

Such developments highlight the critical importance of managing relationships among shareholders for the sustainability of startups. For healthy growth and development within the entrepreneurial ecosystem, shareholder relationships must be carefully managed. In practice, the provisions in shareholder agreements often play a pivotal role in preventing disputes. Key considerations for drafting shareholder agreements to mitigate potential disputes include the following:

- **Transparency:** The legal foundation of shareholder relationships should be solid, and agreements must be clear, detailed, and transparent. These agreements should explicitly define critical elements such as decision-making mechanisms, profit distribution, management rights, and share transfers.

- **Ownership and Decision-Making Rights:** The rights of shareholders and their influence over management should be meticulously structured. Balancing the management rights of majority shareholders with the rights of minority shareholders is essential. Mechanisms should be implemented to prevent majority shareholders from arbitrarily altering decisions to the detriment of minority shareholders.

- **Board Structure:** The independence of the board of directors is crucial in preventing shareholder disputes. Including independent members on the board ensures objective decision-making and minimizes conflicts of interest. Moreover, regular communication of board decisions to shareholders is vital for maintaining transparency.

- **Investor-Entrepreneur Relations:** Investors should focus on long-term sustainability and growth potential rather than short-term profit goals. Shareholder agreements should include mechanisms that prevent investors from making hasty decisions that could hinder the startup's growth trajectory.

- **Dispute Resolution Mechanisms:** Pre-determined dispute resolution methods are essential in case of disagreements among shareholders. Including a clause that requires parties to pursue alternative dispute resolution methods (such as mediation or arbitration) before resorting to litigation ensures faster and more efficient conflict resolution. Additionally, in the event of litigation, it is critically important to determine not only the applicable law but also the jurisdiction in which the proceedings will take place.

In summary, shareholder relations are not only a financial issue but also a strategic concern for startups. Disputes among shareholders underscore how such conflicts can impact not just a single company but the healthy functioning of an entire ecosystem.

Notable Developments in the World of Personal Data

Guide on Cross-Border Personal Data Transfers Published

The eagerly awaited Guide on the Transfer of Personal Data Abroad **(Guide)** was published by the Personal Data Protection Authority **(Authority)** on 2 January 2025.

As known, several changes were made under the 8th Judicial Package to the Personal Data Protection Law **(KVKK)**. Among these changes, new regulations were introduced regarding the transfer of personal data abroad. The Guide provides clarifying explanations regarding these new regulations.

One of the most critical aspects of the Guide was the clarification of the concept of "transfer of personal data abroad." In this regard, the concept is divided into three criteria. Therefore, in order to talk about the transfer of personal data abroad:

- The data controller or data processor (the party transferring the data) must be subject to KVKK for the relevant personal data processing activity.

- The personal data processed by the transferring party must be transmitted or made accessible in some other manner. The Guide provides various examples related to this criterion.

- The data recipient, whether subject to KVKK or not, must be located in a third country.

Additionally, under the new amendments, the Guide outlines a three-tiered transfer regime, including adequacy decisions, appropriate safeguards, and occasional transfers.

You can access the full version of the Guide here *(only available in Turkish)*.

Amendment in the Fundamental Law on Healthcare Services: New Regulations on Processing Health Data

The Law on Amendments to the Social Insurance and General Health Insurance Law and Other Laws was published in the Official Gazette on January 15, 2024, and came into force.

The Law introduced an article titled "Authority to Collect, Process, and Share Information," which includes provisions for the processing of health data to Fundamental Law on Healthcare Services. According to this article, the personal data of individuals who apply to healthcare institutions and health professionals for healthcare services may be processed within the scope of the service.

With this change, a specific regulation regarding personal data was also added to the relevant law. You can access the full version of the law here.

2025 KVKK Administrative Fines Table Published

The Authority has announced the administrative fines applicable under KVKK for 2025.

As a result of violations of decisions by the Personal Data Protection Board, obligations regarding data security, or VERBIS registration obligations, administrative fines ranging from 204,285 TRY to 13,620,402 TRY can be imposed.

You can access the table of administrative fines here.

Banking Sector Best Practices Guide on Personal Data Protection Updated

The Banking Sector Best Practices Guide on Personal Data Protection **(Guide)** has been updated in accordance with the amendments made to the KVKK under the 8th Judicial Package. The Guide aims to direct data controller banks to ensure compliance with KVKK and secondary regulations regarding personal data processing activities and to provide examples of best practices.

Under the Guide, the explanations provided under the heading "Cross-Border Data Transfers" have been aligned with the amendments made to KVKK.

As is known, within the scope of the regulations regarding the transfer of personal data abroad under KVKK, provisions in other laws are explicitly reserved. In this context, the Guide emphasizes that when transferring personal data, which is considered a customer secret, abroad, the provisions of Article 73 of the Banking Law on "Confidentiality of Secrets" and the Regulation on Sharing Confidential Information must be taken into account. The Guide highlights the need to ensure compliance with the changes under KVKK. You can access the full version of the Guide here.

Cooperation Protocol Signed Between the Personal Data Protection Authority and the Capital Markets Board

A cooperation protocol has been signed between the Personal Data Protection Authority and the Capital Markets Board regarding the processing and protection of personal data. The protocol emphasizes that, through this cooperation, joint projects will be undertaken in areas such as data security and protection in the capital markets.

You can access the relevant announcement here.

2024 Annual Activity Information Note Published

The 2024 Annual Activity Information Note was published on the Authority's official website on December 30, 2024.

According to the Note, the Authority concluded 6,958 out of 8,186 notifications, complaints, and applications received in 2024. As a result of investigations conducted under 281 data breach notifications, administrative fines totaling 552 million 668 thousand TRY were imposed. In 2024, the number of notifications regarding the "standard contract" regulations introduced into our legislation for cross-border data transfers was 1,345.

Additionally, the Note provides information on the guides and publications issued by the Authority, awareness and information activities carried out, and steps taken in national and international collaborations. You can access the relevant Note here.

Editors

Görkem Gökçe
gorkem.gokce@gokce.av.tr

Dr. Mehmet Bedii Kaya
bedii.kaya@gokce.av.tr

Elif Aksöz
elif.aksoz@gokce.av.tr

Yağmur Yollu
yagmur.yollu@gokce.av.tr

About us

Gokce Attorney Partnership is an Istanbul-based law firm offering legal services across a broad range of practice areas including mergers and acquisitions, joint ventures, private equity and venture capital transactions, banking and finance, capital markets, insurance, technology, media, telecoms and internet, e-commerce, data protection, intellectual property, regulatory, debt recovery, real property, and commercial litigation. Please visit our web site at www.gokce.av.tr for further information on our legal staff and expertise.

Please contact us at
info@gokce.av.tr
0 212 352 88 33