Legality

"A seminal publication of Şengün Group"

April - May 2025 | E-Bulletin

ŞENGÜN GRUP
Hukuk Law | Medya Media | Strateji Strategy
www. sengungroup.com

ŞENGÜN & PARTNERS
Avukatlık Ortaklığı | Attorney Partnership
www. sengunpartners.com

ŞENGÜN ALSP
Alternatif Hukuk Servis Sağlayıcılığı
Alternative Legal Service Provider
www. sengunalsp.com

APRIL - MAY 2025

LEGALITY

INDEX

Legality
Editor’s Note

Dear Reader,

Şengün Group is delighted to present the April-May 2025 issue of its newsletter that covers the latest local and global developments.

Our articles include “Digital Transformation’s Impact on Personal Data Processing” and “An Analysis of the Operating Principles of Crypto Asset Service Providers Under Recent CMB Regulations”.

This month, our section for the guest sector provides an overview of the national and international dynamics of the technology and IT industries and the relevant legal aspects.

Our article on World Health Day, April 7, addresses awareness-raising activities for individual and public health as well as basic regulations on the right to health.

In our “News to the World” section, we compile the latest regulations, decisions, communiqués, laws, arrangements and amendments regarding national and international relations.

In “World News”, we present global events with transparency as our guiding principle.

Finally, “News from Şengün” reveals the latest developments, events and announcements involving our team.

Enjoy reading!

Istanbul, April-May 2025
Şengün Group

Legality / Editor’s Note

Articles

Article

Digital Transformation's Impact on Personal Data Processing

1) Overview

Today, it is hardly possible to resist technological advancements and their consequences. Indeed, technological progress in every aspect of human existence directly affects the dynamics of our daily lives. In this context, the concepts of digital transformation, compliance and personal data have become highly intertwined. This issue may evolve into a spiral of legal risks in the absence of the right steps.

This article will first discuss digital transformation and its phases from a global perspective, then address the processing of personal data, and finally provide risk and compliance analyses regarding these two basic concepts.

2) Conceptual Analysis

a) What is Digital Transformation?

Although technological progress is often the first thing that springs to mind when it comes to digital transformation, this concept actually refers to progress in socio-economic, cultural, legal and social aspects as well as in technology. Digital transformation should be recognized as a paradigm with impact and consequences on all facets of life. Individuals and institutions have changed their business relations and methods, service delivery, organization, design and models based on this paradigm. Recently, various steps have been taken in relevant areas, such as making data analyses, creating new business lines based on such analyses, and creating a digital world and culture.

Digital transformation can be addressed under the following headings: (i) Data-Driven Approach, (ii) Automation and Artificial Intelligence ("AI"), (iii) Cloud-Based Systems, (iv) Internet of Things (IoT), (v) Mobility and Remote Access, and (vi) Cyber Security and Legal Compliance.

The above-mentioned headings refer to a number of areas that have emerged with the ongoing journey of digital transformation and are the result of years of work and effort. The historical process can be divided into the following periods:

- Early Stages of Digitalization (1950-1980)
- Transition to Information Society (1980-2000)
- Digital Transformation Era (2000-2015)
- Transformation Driven by Data and AI (2015-Present)

Digital transformation has become increasingly widespread and effective over the past decade. In this context, the great change felt in socio-cultural and socio-economic terms has also manifested itself in the field of law. This is because law has a dynamic structure that constantly evolves with the course of life. Affecting all aspects of life, digital transformation has also had a direct impact on people, especially on rights and freedoms.

The relevant developments have influenced many legal disciplines, primarily the Personal Data Protection Law.

b) What Is Personal Data Processing?

The processing of personal data, which is a significant concern for many institutions and organizations, has acquired a new dimension with the emergence of digitalization. In Law No. 6698 on the Protection of Personal Data ("Law No. 6698"), Article 3/1(d) designates personal data as "any information relating to an identified or identifiable natural person". In Article 3/1(e) of the same law, the processing of personal data is defined as follows: "Any operation performed on personal data such as obtaining, recording, storing, retaining, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic means or by non-automatic means provided that they are part of a data recording system".

Article 5 of Law No. 6698 lays down the requirements for personal data processing, and Article 6 defines special categories of personal data that are protected by special measures. Accordingly, special categories of personal data include data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

Since individuals are at the center of the dynamic field of law, definitions and the extent of protection change over time, new categories of data are created, and new obligations are imposed on institutions and organizations that process data.

Pursuant to Law No. 6698, the Personal Data Protection Authority ("Authority") states: "Any operation performed on personal data, such as obtaining, recording, storing, retaining, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic means or by non-automatic means provided that they are part of a data recording system, is accepted as the processing of personal data. All kinds of activities carried out on personal data, from their collection in this manner to their deletion, destruction or anonymization, are considered as processing of personal data under the Law." (https://www.kvkk.gov.tr/Icerik/2048/Kisisel-Verilerin-Islenmesi; accessed 02.04.2025)

The Authority regulates the following in detail: the principles regarding the processing of data at home and abroad; the procedures and principles that multinational companies must comply with when transferring data abroad; the relevant obligations and permissions; the compliance of corporate policies with Law No. 6698 and risk assessments; and the content of standard contracts regarding data transfers. All these processes are kept under control with the Authority's resolutions.

3) Legal Insight with a Risk-Benefit Analysis

Digital transformation leads to the use of digital technologies instead of traditional methods, which, in turn, helps businesses become more efficient, flexible, innovative and competitive. Market players taking advantage of this transformation can review their existing business processes and models to adopt digital technologies and benefit from digitalization capabilities.

Businesses can thus provide goods and services quickly, efficiently, and as expected, while gaining a competitive edge. The progress achieved through effective conditions created by such market players will be followed by various opportunities, including cost savings, innovation and growth, which will accelerate the development process.

Digital transformation is a key strategy for businesses to ensure sustainability and become more competitive in today's rapidly evolving digital world. However, the associated risks should not be ignored. Therefore, data processing undertakings should consider the risks as well as the benefits of digital transformation, as set out below:

BENEFITS OF DIGITAL TRANSFORMATION IN DATA PROCESSING	RISKS OF DIGITAL TRANSFORMATION IN DATA PROCESSING
Increased Efficiency and Accessibility The processing of personal data has become faster and more accurate with automation and AI systems, and access has become easier, especially in public services.	**Risk of Privacy Breaches** The vulnerability of digital systems to cyber-attacks has increased threats such as identity theft, unauthorized access and data leakage.
Data-Driven Decision Making Thanks to big data and analytics systems, more effective decision-making processes that draw meaningful conclusions from personal data have been developed.	**Excessive Data Collection** The conveniences offered by technological means can cause data to be collected and stored in a way that is often not aligned with the intended purpose.
Transparency and Accountability Digital monitoring and recording systems developed to comply with regulations such as Law No. 6698 and the GDPR have increased the transparency of data controllers' activities.	**Weakening of Anonymization** There is a risk that previously anonymized data can be re-identified with advanced algorithms.
Effective, Fast and Solution-Oriented Service and Goods Delivery Strategies Competition has been increased to raise the added values of market players and to ensure the upward movement of the free market economy, thus supporting the market without leading to anti-competitive conduct.	**Algorithmic Decisions and Discrimination** Automated decision-making systems can have negative impacts on individuals and cause discrimination if they are not sufficiently transparent.

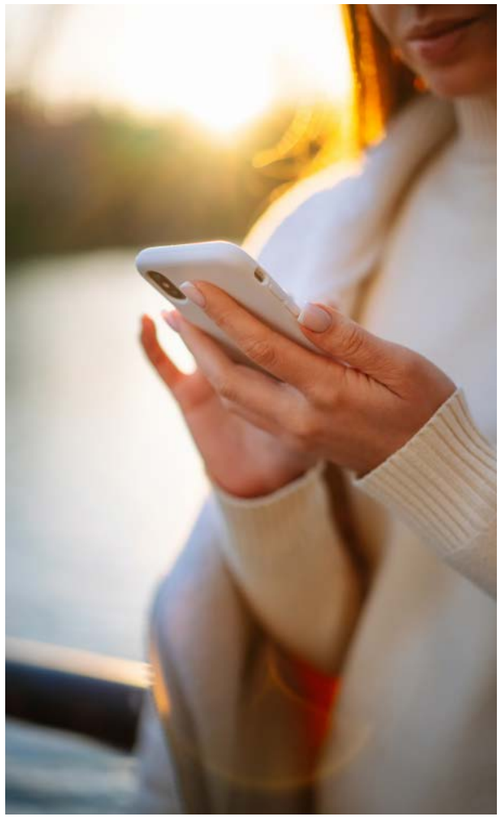
In this context, it could be useful to review a number of international risk assessments. In cases involving digital data processing, the European Court of Human Rights ("ECHR") often refers to Article 8 "Right to Respect for Private and Family Life" and Article 10 "Freedom of Expression" in the European Convention on Human Rights to pass its infringement judgments.

In PODCHASOV v. RUSSIA (application no. 33696/19, 13.02.2024), which is deemed a landmark case, the ECHR concluded as follows (https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-230854%22]}; accessed 03.04.2025):

In the relevant case, the applicant is a user of Telegram, an application that uses a custom-built server-client encryption scheme in its default "cloud chats". However, it is possible to switch to end-to-end encryption by activating the "secret chat" feature. The applicant uses the application by activating "end-to-end encryption". On 28 June 2017, Telegram Messenger LLP was listed as an "Internet communications organiser" (организатор распространения информации в сети Интернет – hereinafter "ICO") in a special public register.

This entailed an obligation for Telegram to store all communications data for a duration of one year and the contents of all communications for a duration of six months, and to submit those data to law-enforcement authorities or security services in circumstances specified by law, together with information necessary to decrypt electronic messages if they were encrypted. Due to this obligation, on 12 July 2017, the Federal Security Service ("FSB") requested Telegram Messenger LLP to disclose even users' encrypted communications. In response to this, the plaintiffs argued that the provision of encryption keys as required by the FSB would enable the decryption of the communications of all users. It would therefore breach their right to respect for their private life and for the privacy of their communications.

In this case, the ECHR referred to international legislation to reach a decision regarding digital breaches of personal data. Indeed, one may find significant principles in international legislation.



Accordingly:

i. The Report on the Right to Privacy in the Digital Age by the Office of the United Nations High Commissioner for Human Rights, published on 4 August 2022 (A/HRC/51/17) reads as follows: Encryption is a key enabler of privacy and security online and is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly, security, health and non-discrimination. It is essential if people are to feel secure in freely exchanging information with others on a range of experiences, thoughts and identities, including sensitive health or financial information, knowledge about gender identities and sexual orientation, artistic expression and information in connection with minority status. In environments of prevalent censorship, encryption enables individuals to maintain a space for holding, expressing and exchanging opinions with others. This right could be limited only when it is proven beyond doubt that it is necessary to meet a particular legitimate interest.

ii. Recommendation by the Committee of Ministers of the Council of Europe on the protection of human rights with regard to social networking services (CM/Rec(2012)4, adopted on 4 April 2012) reads as follows: In co-operation with the private sector and civil society, member States, in addition to the measures stated in section I of this appendix, should take appropriate measures to ensure that users' right to private life is protected, in particular by engaging with social networking providers to carry out the following actions...

iii. The Council of Europe Parliamentary Assembly Resolution 2045 (2015) on mass surveillance, adopted on 21 April 2015, reads as follows: The Assembly therefore urges the Council of Europe member and observer States to ensure that their national laws only allow for the collection and analysis of personal data (including so-called metadata) with the consent of the person concerned or following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity; unlawful data collection and processing should be penalised in the same way as the violation of the traditional confidentiality of correspondence; the creation of 'back doors' or any other techniques to weaken or circumvent security measures or exploit their existing weaknesses should be strictly prohibited; all institutions and businesses holding personal data should be required to apply the most effective security measures available.

iv. The judgment given by the Court of Justice of the European Union (CJEU) on 8 April 2014 in the joined cases of Digital Rights Ireland and Seitinger and Others (C-293/12 and C-594/12, EU:C:2014:238) declared the Data Retention Directive 2006/24/EC invalid. The Directive laid down an obligation on the providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data for periods from six months to two years, in order to ensure that the data were available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each member State in its national law. (For relevant case-law, see Big Brother Watch and Others v. the United Kingdom [GC], no. 58170/13).

v. A Joint Statement by Europol and the European Union Agency for Cybersecurity (ENISA) of 20 May 2016 on lawful criminal investigation that respects 21st Century data protection reads as follows: Intercepting an encrypted communication or breaking into a digital service might be considered as proportional with respect to an individual suspect, but breaking the cryptographic mechanisms might cause collateral damage. The focus should be on getting access to the communication or information; not on breaking the protection mechanism. (...) yet access to encrypted information is imperative for security and justice, then feasible solutions to decryption without weakening the protective mechanisms must be offered, both in legislation and through continuous technical evolution. For the latter, the fostering of close cooperation with industry partners, as well as the research community with expertise in crypto-analyses for the breaking of encryption where lawfully indicated, is strongly advised.

vi. On 28 July 2022, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) adopted Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. It reads as follows, in so far as relevant: The EDPB and EDPS point out that encryption technologies contribute in a fundamental way to the respect for private life and confidentiality of communications, freedom of expression as well as to innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide. European data protection authorities have consistently advocated for the widespread availability of strong encryption tools and against any type of backdoors. This is because encryption is important to ensure the enjoyment of all human rights offline and online. Moreover, encryption technologies contribute in a fundamental way both to the respect for private life and confidentiality of communications. In the context of interpersonal communications, end-to-end encryption ("E2EE") is a crucial tool for ensuring the confidentiality of electronic communications, as it provides strong technical safeguards against access to the content of the communications by anyone other than the sender and the recipient(s), including by the provider. Preventing or discouraging in any way the use of E2EE, imposing on service providers an obligation to process electronic communication data for purposes other than providing their services, or imposing on them an obligation to proactively forward electronic communications to third parties would entail the risk that providers offer less encrypted services in order to better comply with the obligations, thus weakening the role of encryption in general and undermining the respect for the fundamental rights of European citizens. Thus, their use should not be prevented or discouraged.

Following all this international review in PODCHASOV v. RUSSIA, the ECHR concluded as follows: The contested legislation providing for the retention of all Internet communications of all users, the security services' direct access to the data stored without adequate safeguards against abuse and the requirement to decrypt encrypted communications, as applied to end-to-end encrypted communications, cannot be regarded as necessary in a democratic society. In so far as this legislation permits the public authorities to have access, on a generalised basis and without sufficient safeguards, to the content of electronic communications, it impairs the very essence of the right to respect for private life under Article 8 of the Convention. The respondent State has therefore overstepped any acceptable margin of appreciation in this regard. There has accordingly been a violation of Article 8 of the Convention.

In some of its rulings, the Turkish judiciary also recognized that the content of communications was personal data and emphasized the need for their protection. For instance, the 9th Civil Chamber of the Court of Appeals designated WhatsApp communications as personal data and reminded their protected status in Decision No. 2019/559, File No. 2018/10718, 10.01.2019.

The decision reads as follows: "WhatsApp enables mobile communication via the Internet. Using this application, one can communicate individually or in groups with other users. However, this system is protected with end-to-end encryption. (...) these communications must be protected as personal data."

The Criminal General Assembly of the Court of Appeals held a similar opinion in Decision No. 2014/331, File No. 2012/12-1510, 17.06.2014, which reads as follows: "Articles 135 and 136 of the Turkish Criminal Code do not stipulate that only confidential personal data will be protected. On the contrary, the justification of Article 135 states that all kinds of information on a real person should be considered as personal data. Accordingly, it should be accepted that the acts of unlawful transfer, dissemination and seizure of all kinds of personal data constitute the crime stipulated in Article 136 of the Code. (...) Thus, the action in question constitutes the crime of unlawful dissemination of personal data regulated in Article 136 of the Code."

Digital transformation opens up a wide and effective space that contributes significantly to socio-economic aspects and accelerates development. However, when the transformation's legal dimension is inquired, especially within the framework of fundamental human rights, it is seen that a number of rights related to personal data are affected. The scope, nature and value of personal data are directly related to various human rights, and the slightest legal deficiency or breach in this regard may lead to serious violations of such fundamental rights.

4) Conclusion

While digital transformation provides significant convenience and benefits in the processing of personal data, it also imposes serious obligations for data security. Data controllers and processors, who are legally bound in this regard, should act in compliance with Law No. 6698 and within an ethical framework when using digital technologies and continuously update their risk analyses. Otherwise, they may harm individuals' fundamental rights and freedoms and face serious sanctions.

Gülşah Güven, LL.M., Partner

Legality / Articles

Article

An Analysis of the Operating Principles of Crypto Asset Service Providers Under Recent CMB Regulations

The crypto assets market has turned into a key component of the global financial system in recent years. In Türkiye, the Capital Markets Board ("CMB") published Communiqué No. III-35/B.1 on the Establishment and Operating Principles of Crypto Asset Service Providers and Communiqué No. III-35/B.2 on the Operating Procedures and Principles and Capital Adequacy of Crypto Asset Service Providers in Official Gazette No. 32840 of 13.03.2025 to address the regulatory gap in this area.

The Communiqué on the Establishment and Operating Principles of Crypto Asset Service Providers (III-35/B.1) concerns the following aspects: requirements for the establishment of crypto asset service providers ("CASPs"), qualifications required for founders and shareholders, procedures for obtaining operating permits, organizational and technological infrastructure obligations, share transfers, provisions on suspension or limitation of activities, and administrative sanctions.

The Communiqué on the Operating Procedures and Principles and Capital Adequacy of Crypto Asset Service Providers (III-35/B.2) regulates the following issues among others: services and activities that CASPs may offer, listing principles, settlement and custody system, capital adequacy requirements, limitations on investment advisory, and prohibited transactions.

I. Requirements for Establishment and Operating Permit

CASPs must be established as a joint stock company. The shares must be registered and issued against cash, the founding capital must not be below the minimum amount defined by the CMB and must be fully paid in cash, and the stockholders' equity must not be less than this amount.

Founders must not be bankrupt, have declared concordat, been convicted of disgraceful crimes, or held responsible for companies with revoked authorizations. In addition, the shareholding structure should be transparent and open.

In their trade names, CASPs must include phrases that clearly indicate their field of activity. Accordingly, the title of a platform must include the phrase "crypto asset trading platform", whereas the title of a custodian must include the phrase "crypto asset custodian".

CASPs must apply for an operating permit within 6 months after obtaining an establishment license from the CMB. They must have completed the necessary technical and administrative preparations during that time. Otherwise, the establishment license will become null and void.

In order to obtain an operating permit, CASPs must meet the following criteria:

- The requirements for establishment must still be satisfied.
- The minimum founding capital must be paid in cash and in full.
- The capital adequacy obligations under the CMB's regulations must be fulfilled.
- An organizational structure must be in place.
- The requirements for the personnel, general manager and deputy general managers must be fulfilled.
- The necessary security infrastructure must be established and maintained.
- Units, systems and functions for internal audit, control and risk management must be established.
- The necessary technical and system integration tests must be completed with the Central Securities Depository and Trade Repository of Türkiye ("MKK").
- The infrastructure for storing private keys must be in place, secure and integrated with distributed ledger networks.

Once all these conditions are met, the CMB may conduct on-site inspections or have third parties conduct information systems audits.

II. Operating Principles and Guidelines

CASPs must comply with the general principles and guidelines stipulated in the first paragraph of Article 24 of Communiqué No. III-39.1 on Guidelines for the Establishment and Operations of Investment Companies.

CASPs must be a member of the Capital Markets Association of Türkiye.

Customers should be informed about the general risks posed by crypto assets through a form with the minimum content required by the CMB, and a written or electronic statement indicating that they understand those risks should be obtained from them. The disclosures must also include information on the following matters: all types of commissions, fees, and tax amounts or rates related to the transactions; where the customer's crypto assets and cash are held; information on the market maker and liquidity provider, if any; and whether customer transactions have a counterparty. This information should be provided using specific and quantifiable examples, rather than general statements.

Platforms must sign a framework contract with their customers before processing transactions with them. This contract can be concluded electronically and constitutes the legal framework that defines the relationship between the platform and the customer and forms the basis for individual transactions. In addition to the parties' rights and obligations, the contract must at least set out transaction processes, fees and commissions, custody procedures and security provisions.

Under the legislation on anti-money laundering and combating the financing of terrorism, it is obligatory to comply with the principles of identity verification and Know Your Customer (KYC). Remote identity verification can be used in customer acquisition, with the resulting information secured through verification via an official population database. In addition, the persons who will carry out transactions on behalf of the customer must be authorized with a special power of attorney issued by a notary public, and their identity must also be verified in accordance with the relevant legislation.

CASPs are required to disclose their authorized services and introductory information on the Public Disclosure Platform (KAP) and on their websites. Introductory information about the company should at least provide the following: trade registry information, latest shareholding and management structure, telephone number, corporate address, e-mail address and annual reports. (Communiqué No. III-35/B.1 specifies the minimum information required to be provided on the websites of platforms and custodians.)

III. Services and Activities That CASPs May Offer

- Receiving, executing and clearing crypto asset orders, transferring crypto assets, and offering custody services,
- Brokering the initial sale or distribution of crypto assets,
- Storing and managing crypto assets or private keys related to those assets or offering other custody services to be determined by the CMB,
- Providing investment advisory for crypto assets,
- Offering other services and activities to be defined by the CMB.

NFT transactions and crypto asset financial analysis services can also be provided after notifying the CMB, without an authorization certificate.

IV. Prohibited Activities and Restricted Transactions

CASPs may only engage in the activities authorized by the CMB and are prohibited from conducting any other industrial or agricultural activities. Prohibited activities include guaranteeing returns, conducting unauthorized transactions, conducting transactions on behalf of a customer with comprehensive powers of attorney, trading in foreign currency, or transferring foreign currency abroad.

It is also prohibited to use crypto assets in leveraged transactions, derivative contracts, credit trading or lending transactions.

Yiğit Okuldaş, Executive Associate

Guest Sector

Guest Sector

Technology and IT Industries

The industries of technology and IT (information technology) are evolving rapidly worldwide, turning into key elements that redefine economic and social structures. Both developed and developing countries are increasing their investments in these industries while creating or monitoring innovations.

Due to the size, potential and unique characteristics of these industries, new regulations and legal strategies are needed to address emerging issues.

Regulations affecting the technology and IT industries do not only concern the establishment of technical infrastructure. There are also important regulations affecting economic, social and cultural dynamics.

This article will first provide an overview of the industries and then address the relevant legal considerations.

Legality / Guest Sector

A) Characteristics and Importance of Technology and IT Industries

The technology and IT industries draw attention with their ever-changing features as business areas at the center of modern economies. Globally, these industries are among the top ten sectors with a market volume worth several trillion dollars.

The technology industry is growing each year across the world, driven by digital transformation, increased data consumption, the proliferation of cloud computing services and the growing impact of artificial intelligence applications. With technological developments, the IT and telecommunications industries have become intertwined. Therefore, if these two industries are treated as a single industry, an even larger market volume will be seen.

Türkiye is among the countries with significant growth potential in the technology and IT industries. In the country, the main IT areas that are rapidly developing with significant growth potential include software and game development, e-commerce and fintech.

From a market perspective, the US seems to be leading the global technology race. Still, some EU countries and Türkiye continue to offer opportunities for entrepreneurs and startups working in technology and IT. This creates an ecosystem where smaller and innovative companies can still have a presence in the market, alongside tech giants. However, to protect this limited ecosystem in the face of various advantages enjoyed by giant corporations, there is a need for rigorous regulations and high sensitivity in administrations' inspections and audits.

B) Legal Aspects of Technology and IT Industries

Constantly undergoing rapid changes, the technology and IT industries also create specific circumstances in terms of regulations. Technological innovations should be shaped in parallel with legal regulations, both in Türkiye and around the world.

As such, lawmakers' failure in keeping up to date with technological advancements may create difficulties for consumers. On the other hand, legal restrictions before due time can hinder initiatives. The main legal areas regarding the technology and IT industries will be outlined below.

1. Electronic Communications Regulations and Access Bans

In a rapidly digitalizing world, the laws on access bans and data security are crucial for the regulation of the electronic communications sector. In the field of electronic communications, access bans imposed by state regulatory authorities play a vital role, especially in the prevention of cybercrimes.

In Türkiye, institutions such as the Information and Communication Technologies Authority ("ICTA") regulate this field to ensure the security of users. Significant regulations include Law No. 5809 on Electronic Communications, Law No. 5651 Regulating Online Content and Fighting Crimes Committed Through Such Content, and the regulations enforced by the ICTA.

From a legal perspective, these regulations need to strike a balance between freedom and security without hindering the development of the sector. In order for individuals and news sources to know their boundaries within which they can express themselves freely in an electronic environment, the relevant regulations and penalties should fulfill the criterion of certainty.

2. E-Commerce: Compliance and Oversight

E-commerce has grown rapidly in Türkiye and across the world in recent years. This growth, in return, has increased the importance of a legal framework for e-commerce activities. Key legal concerns include consumer rights, the validity of digital contracts, and the security of payment systems.

Regulations such as Law No. 6563 on the Regulation of Electronic Commerce, the Regulation on Distance Contracts, Law No. 7223 on Product Safety and Technical Regulations and the Regulation on Market Surveillance and Inspection of Products Introduced to the Market via Remote Communication Tools issued based on this law, and the Framework Regulation on Market Inspection and Surveillance of Products encourage all market players to act in compliance.

3. Sustainability

Sustainability is becoming more important each day with the rapid advancement of technology. Environmental sustainability and economic sustainability have turned into the determinants of the future of the technology and IT industries. As such, regulations are rapidly being introduced to reduce the negative environmental impact of these industries and to use resources more efficiently while guiding the industries in this respect.

In Türkiye, the Regulation on Ecodesign of Energy-Related Products, which entered into force in 2022, constitutes an important step in reducing environmental impacts of the technology and IT industries in the country.

On March 21, 2025, the ICTA announced a public consultation period for (i) the Draft Communiqué on Ecodesign Requirements for Smartphones, Feature Phones, Cordless Phones and Tablets and (ii) the Draft Communiqué on Energy Labels of Smartphones and Tablets. Scheduled to be effective June 20, 2025, these communiqués will become significant regulations for sustainability in the relevant industries if formally enacted.

While protecting consumers and the environment, these types of regulations also promote more efficient and sustainable production processes. As environmental sustainability is not an isolated issue, these regulations will also provide long-term economic and social benefits for the technology and IT industries.

4. Compliance and Regulation: Fintech, RegTech and Crypto Assets

Developments in fintech, RegTech and crypto assets profoundly affect the financial sector and the relevant regulations and are also closely linked to the technology and IT industries. Cryptocurrency markets are not yet fully regulated worldwide, which creates legal gaps and poses serious challenges in combating crimes such as fraud and money laundering, especially in some countries. As of 2025, Türkiye has made significant progress in the regulation of crypto assets with ongoing regulations. In this respect, it is crucial to eliminate all legal uncertainties in the sector and to adopt regulations that are feasible and compatible with technological advancements.

However, except for data protection, crypto assets and financial aspects, Türkiye has almost no regulations directly addressing areas such as web3, blockchain and smart contracts. In some European countries and the US, regulatory authorities are making efforts to monitor the risks more closely. Nevertheless, the ongoing regulatory efforts are still limited and at an early stage.

5. Competition Law and Anti-Competitive Practices

Since competition is fierce in the technology and IT industries, competition law plays a critical role in these sectors. It is often observed that technology giants attempt to dominate the market, engage in anti-competitive behaviors, put themselves at an advantage and exclude competitors, thus leading to unfair competition.

Despite various incentives, it is very difficult for a startup to survive and compete against vertically integrated giant companies with huge financial means and big data, as the playing field is not level across the globe. With the recent trend of acqui-hiring, startups that are lucky enough to make an impact with their innovations are being acquired by large companies, and their talent is being transferred to them. In Türkiye and around the world, regulations and investigations in this field are crucial to ensure checks and balances in the sector.

6. Personal Data Protection and Data Privacy

Concepts such as data security, personal data protection and user rights are becoming more important each day with the increasing impact of digitalization. In Türkiye, Personal Data Protection Law No. 6698 has been a key regulation for the protection of users' personal data. In this context, there are significant legal obligations that IT companies must comply with in their data processing processes.

In addition to the lawful and limited processing of data in line with the intended purposes, the issue of data transfer to other countries is also important in an era of increased cloud usage. Arguably, the most significant problem is that even in organizations such as government agencies and Internet providers, which are entrusted with citizens' sensitive personal data, the data may not be fully secure.

Legality / Guest Sector

7. Entrepreneurship and Startup Incentives

Entrepreneurs and startups are the drivers of innovation in the technology and IT industries. Türkiye offers various legal incentives and tax advantages to support entrepreneurship, especially under Law No. 5746 on Supporting Research, Development and Design and Law No. 4691 on Technology Development Zones. For the effective use of such incentives, entrepreneurs should be informed about the regulations that apply to them.

Other significant advantages include 80% tax exemption granted to software exporters under Corporate Tax Law No. 5520 and Income Tax Law No. 193, and exemption up to a certain amount granted to full taxpayer real persons under the age of 29 for three tax periods as per the Income Tax Law. Likewise, the revenues of software developers, programmers and inventors from their own works through publishing, sale, transfer or lease are also exempt from income tax.

8. Intellectual and Industrial Property Rights

The technology and IT industries present a complicated picture for intellectual and industrial property rights, with patents, trademarks, designs and utility models being critical for technology companies. The undertakings operating in these industries can contribute to the protection of innovations by safeguarding their own rights and not infringing the intellectual and industrial property rights of others. In the field of industrial property, the state has programs to support entrepreneurs' expenditure. The relevant incentives include the 1602 TÜBİTAK Patent Support Program, KOSGEB Industrial Property Rights Support, and exemption from corporate tax and VAT on industrial property rights.

9. Criminal Law

Rapid developments in the technology and IT industries have facilitated the commission of certain illegal activities and made them more difficult to detect. Therefore, new regulations have emerged to combat them. While some crimes are specific to this field, the commission of other offenses in the digital environment also constitutes a major form of criminal activity in a number of cases. Cybercrime is a broad concept used for all kinds of criminal activities committed in the digital environment.

In Türkiye, under Articles 243 to 245 of Turkish Criminal Code No. 5237, titled Cybercrimes, the listed crimes are (i) access to information systems, (ii) hindrance or destruction of systems, deletion or alteration of data, (iii) misuse of bank or credit cards, and (iv) prohibited devices or programs. In addition, crimes such as violation of the privacy of communications/ private life, unlawful delivery or acquisition of data, and failure to destroy data, which are regulated under the title Crimes Against Privacy and Secrecy of Life, are also closely related to the areas of IT and technology. Cybercrimes also include financial offenses such as aggravated fraud, qualified theft, and facilitating illegal gambling. The commission of some capital market crimes may also involve the use of technological means. Despite the difficulty of identifying the perpetrator, cybercrimes can lead to significant criminal sanctions.

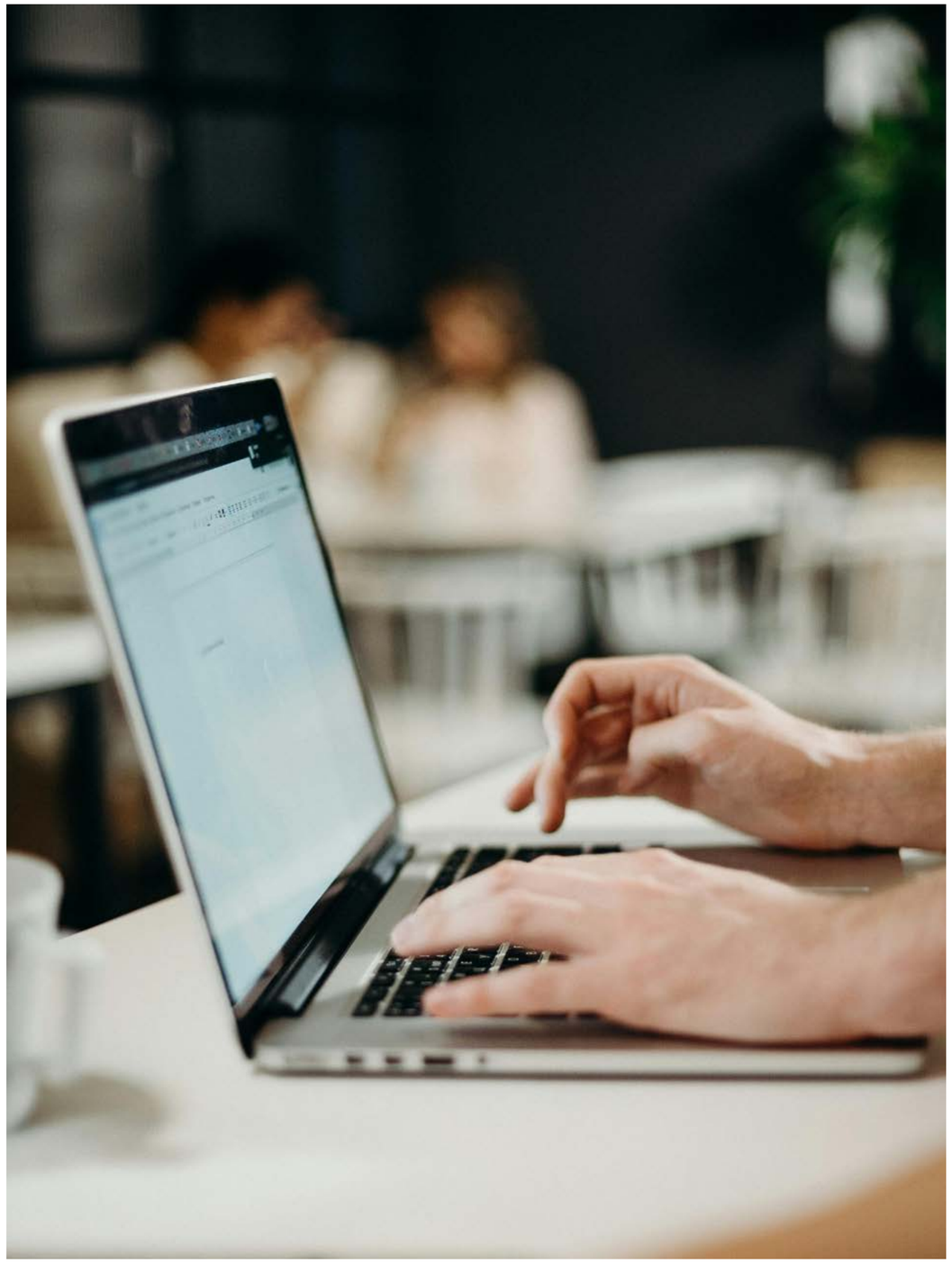
Conclusion

Technology and IT industries are crucial for both economic growth and regulations with their rapidly evolving dynamics. The relevant regulations in Türkiye and worldwide directly affect the activities of market players.

Therefore, it is essential for technology and IT professionals to comply with the regulations and closely follow the developments regarding these industries. The proper application of legal knowledge by entrepreneurs and other stakeholders is crucial to their success and essential for fostering healthy and secure growth in the technology and IT industries.

İdil Aşkın, Associate

Legality / Guest Sector



Special Day

Special Day
World Health Day, April 7

April 7, the date on which the World Health Organization (“WHO”) Constitution came into force, is celebrated as “World Health Day” every year across the world. The day aims to raise awareness about individual and public health, with worldwide activities offering solutions and suggestions related to the annual health theme chosen by the WHO. The theme for 2024 was “My health, my right”, which drew attention to the right to health, while the theme for 2025 is “Healthy beginnings, hopeful futures”.

According to the recent reports and data on this year’s health theme, approximately 300,000 women die during pregnancy and childbirth, more than 2 million babies die in the first month after birth, and almost 2 million babies are stillborn worldwide. Thus, this year’s theme underscores the need to prioritize and protect the long-term health of mothers and babies for building healthier families and societies.

Legality / Special Day

Key International Regulations on the Right to Health

The Universal Declaration of Human Rights (“Declaration”), arguably the most critical document in the history of human rights, contains universal and fundamental provisions on the right to health and on this year’s World Health Day theme. In the Declaration, Article 25 sets out that everyone has the right to a standard of living adequate for the health and well-being of themselves and of their family, adding that “Motherhood and childhood are entitled to special care and assistance. All children, whether born in or out of wedlock, shall enjoy the same social protection.” Thus, the Declaration underlines and recognizes the right to health for mothers and children as a fundamental human right.

The Constitution of the World Health Organization (“Constitution”), which was the source of inspiration for World Health Day, is a fundamental regulation that lays down various principles that require the signatories to protect public health. The Constitution aims to achieve the highest attainable standard of health for all nations. To this end, various efforts are undertaken to strengthen international healthcare services, to carry out healthcare activities and to promote health and safety.

The Constitution contains significant provisions for this year’s World Health Day theme. In line with the Declaration, the States that are bound by the Constitution accept the principle that “Healthy development of the child is of basic importance; the ability to live harmoniously in a changing total environment is essential to such development.” Likewise, paragraph l of the second article, which regulates the duties of the WHO, stipulates that one of the functions of the WHO will be “to promote maternal and child health and welfare and to foster the ability to live harmoniously in a changing total environment.”

In conformity with the Constitution, another important regulation containing norms and provisions for universal observation of the right to health is the International Health Regulations ("IHR"). The IHR aims to prevent, protect against, control, and provide a public health response to the international spread of disease in ways that are commensurate with and restricted to public health risks.

Conclusion

As commonly accepted, health is not merely the absence of disease or physical impairment, but a holistic state of physical, mental, and social well-being. The right to health is a fundamental and universal right for every human being, regardless of race, religion, political belief, economic and social conditions. It extends beyond individuals, with far-reaching social and communal implications. Indeed, the health of a society depends on the well-being of its core elements, the individuals. However, for individual and public health, an accessible, transparent and equal health system is essential along with the meticulous work of healthcare providers.

In the context of the right to health of individuals and communities, the well-being of mothers and babies/children deserves special emphasis. The health of the institution of family, arguably the most organic and fundamental bond between the individual and the society, is also crucial for achieving collective health. However, the well-being of families and the exercise of the right to health depend on the health of mothers and children. Indeed, the existence of a healthy society is impossible when mothers and children cannot exercise the right to health functionally, adequately, appropriately or at all. Therefore, as emphasized by the theme of this year's World Health Day, women and families worldwide must be afforded physical and emotional support along with quality care during and after childbirth.

Ahmet Oğul Aksoy, Associate

Legality / Special Day

News to the World

Legality
News to the World

Legality / News to the World

Law Amending the Law on Youth and Sports Services and Certain Laws and Decree-Laws

With the completion of the negotiations on the second part of the Bill of Law Amending the Law on Youth and Sports Services and Certain Laws and Decree-Laws, some arrangements were enacted into law and entered into force. The Law Amending the Law on Youth and Sports Services and Certain Laws and Decree-Laws ("Law") was published in Official Gazette No. 32857 of 30.03.2025. Accordingly:

In order to prepare for the Olympic, Paralympic and Deaflympic Games every summer and winter, 8 thousand athletes will be trained in Olympic, Paralympic and Deaflympic sports. The Ministry of Youth and Sports will cover the athletes' nutrition, accommodation and travel expenses. Payments will be free of taxes and deductions and will not be sequestrated.

Furthermore, additional Article 4 of Decree-Law No. 633 was amended. Accordingly, for children born after 1 January 2025 of Turkish citizens residing in Türkiye, the following maternity allowances will be granted: "one-time ₺5,000 for the first child, ₺1,500 per month for the second child from the month of application until the child reaches the age of 5, and ₺5000 per month for the third and subsequent children from the month of application until they reach the age of 5 (including the sixtieth month)." Maternity allowances will be free of taxes and deductions and will not be sequestrated.

The Law also increased the amount of the retirement bonus specified in Law No. 5510 from ₺3,000 to ₺4,000.

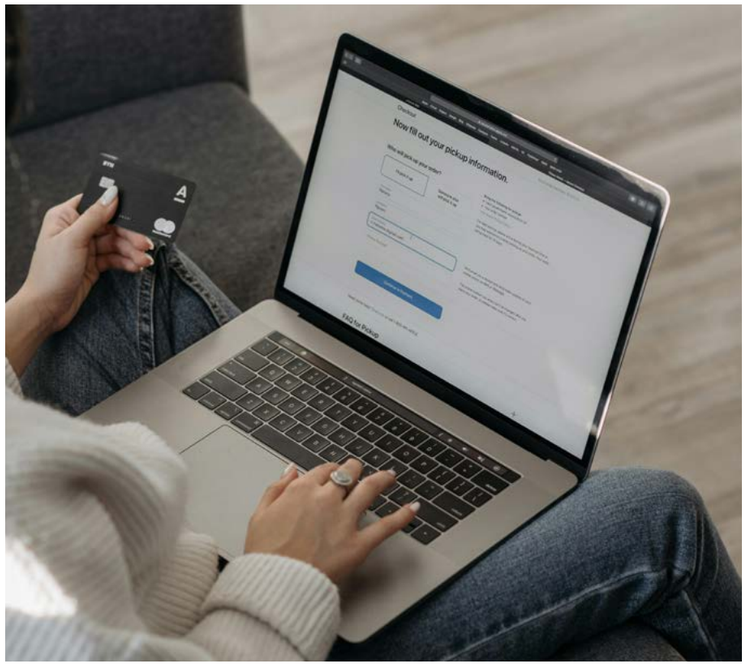
See the full Law at:

https://www.resmigazete.gov.tr/eskiler/2025/03/20250330-1.htm

Amendments to the E-Commerce Regulation

The Regulation Amending the Regulation on Electronic Commerce Intermediary Service Providers and Electronic Commerce Service Providers ("Amendments"), published in Official Gazette No. 32835, made significant changes to the Regulation on Electronic Commerce Service Providers ("Regulation").

First, the obligation for electronic commerce service providers ("ECSPs") to provide certain information about themselves has been abolished. Previously, ECSPs were obliged to provide a registered email address (KEP) or their full name, depending on whether they were merchants. This obligation is no longer applicable. Electronic commerce intermediary service providers ("ECISPs") must verify the information provided by ECSPs once a year. While this verification was required within the first three months of each year previously, a once-a-year verification will now be sufficient.



Regulations on unfair commercial practices have also been expanded. From now on, ECISPs will be entitled to extend withdrawal periods in intermediation agreements without the consent of ECSPs. In addition, imposing penalties via an internal communication system will be considered an unfair commercial practice. With another amendment regarding intermediation agreements, the 15-day period will be waived for agreement amendments that will benefit ECSPs, provided that they are notified in advance. The obligation to update inventory details has been abolished for ECSPs providing catering services.

Advertising and discount budgets have also been amended. Sponsorship expenditure was previously allowed up to 25% of advertising expenditure. Now, it is allowed up to 50%. In addition, discounts for outreach will be excluded from the discount budget. Sales overseas will be exempt from the license fee calculation, with the introduction of new rules. ECISPs will be obliged to verify foreign sales. Medium and large-sized ECSPs and ECISPs will have to submit their independent audit reports to the Ministry in August each year. Likewise, compliance reports will be submitted in August.

See the full Regulation at:

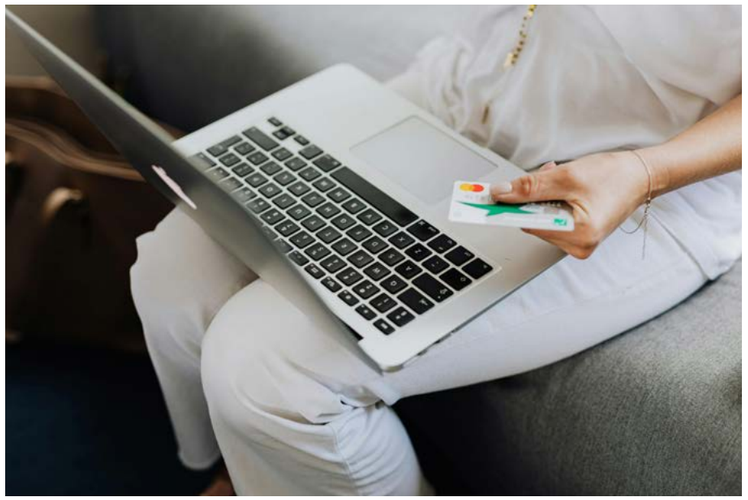
https://www.resmigazete.gov.tr/eskiler/2025/03/20250308-1.htm

Regulation on Market Surveillance and Inspection of Products Introduced to the Market via Remote Communication Tools Enters into Force

The Regulation entered into force on April 1, 2025, upon publication in Official Gazette No. 32707. Under the Regulation, product detail pages must include the required warning and safety information in Turkish. Thus, online shoppers will view products and evaluate them based on the necessary markings.

If a website is found to be selling non-compliant products, the relevant product detail pages must be removed within 24 hours. If the page is not removed within this period, access to it will be blocked.

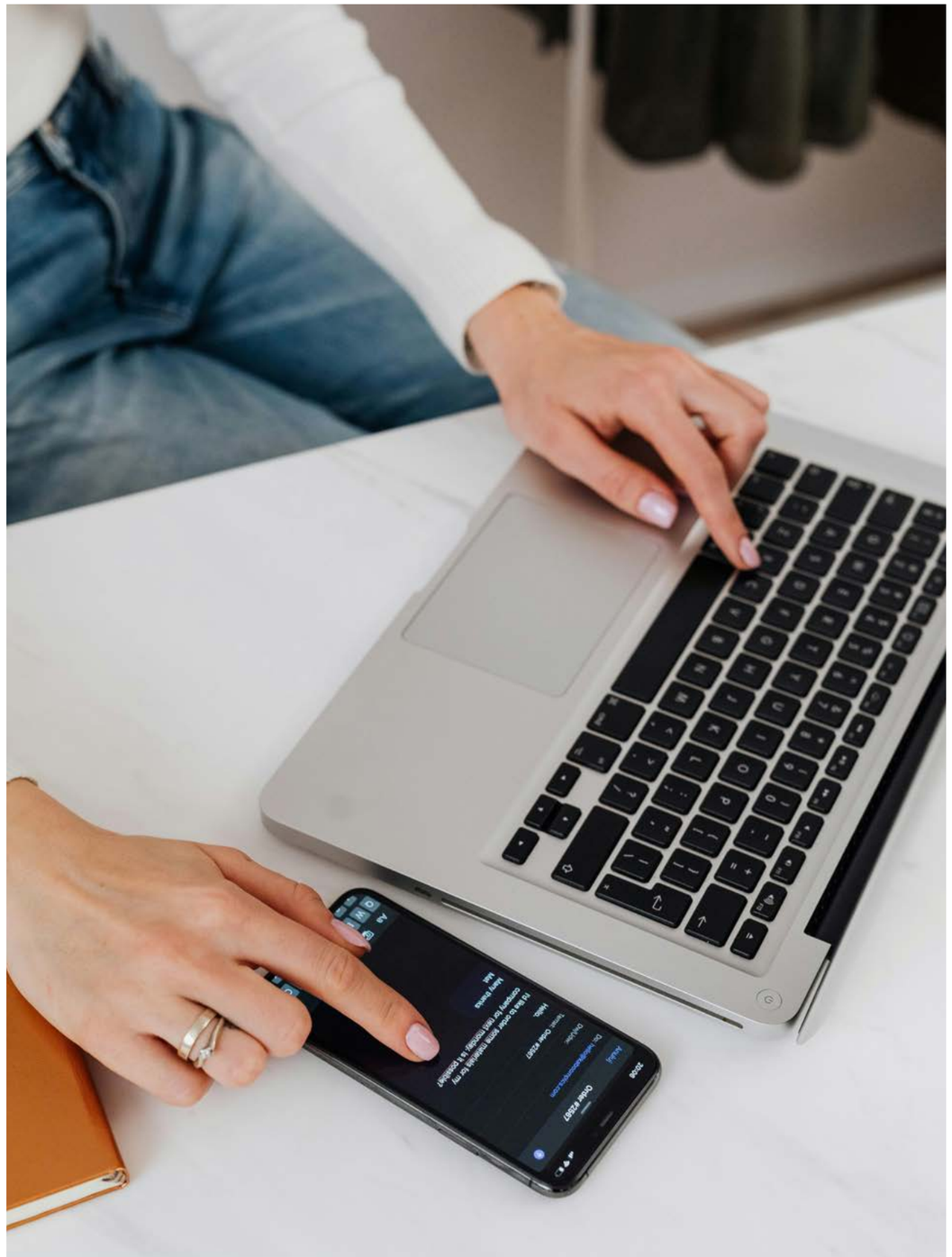
Sales platforms will establish a “product safety contact point”. Through this contact point, customers will be able to raise complaints about product safety and compliance. In addition, the presence of an economic operator resident in Türkiye is now obligatory for certain products.



See the full Regulation at:

https://resmigazete.gov.tr/eskiler/2024/10/20241030-2.htm

Legality / News to the World



World News

Legality
World News

Legality / World News

Burger King Faces Lawsuit Over Allegedly Misleading Ads

Burger King faces a class action lawsuit in the US state of Miami for allegedly misleading consumers with advertisements that make its Whopper sandwich and other menu items appear larger than they are, on the grounds that some consumers may be deceived by these ads. U.S. District Judge Roy Altman considered the plaintiffs' claims that Burger King materially overstated the size of its products in photos and found that these ads could be misleading for some reasonable consumers.

Nineteen customers from 13 states claimed that Burger King overstated the size of its menu items, with the Whopper appearing 35% larger than the actual burger and containing more than double the meat. Burger King, on the other hand, acknowledged that the photos were designed by professional photographers, arguing that the point of these ads was to make products appear as appetizing as possible. However, Judge Altman found that these ads went beyond "mere exaggeration".

Unlike similar actions against McDonald's and Wendy's, the lawsuit focuses on the allegation that Burger King started making the Whopper appear bigger in post-2017 ads. Toronto-based Restaurant Brands International, the parent company of Burger King, said in a statement regarding the lawsuit, "The plaintiffs' claims are false," adding that the flame-grilled beef patties portrayed in the ads were the same patties served in restaurants.

While Anthony Russo, a lawyer for the plaintiffs, expressed satisfaction with the court decision, a similar lawsuit against Subway is pending in the Brooklyn court.

Judge in Meta Case Says AI Can Obliterate Market for Original Works

A federal judge in San Francisco questioned the argument that copyrighted works can be used legally without permission to train artificial intelligence (“AI”) models.

The judge told Meta’s attorneys that they had companies using copyright-protected material to create a product that was capable of producing an infinite number of competing products. Stating that the company might be dramatically changing the market for a person’s work, even without paying a license or compensation to that person, the judge argued that this could not be fair use.

The legal doctrine enables companies such as Meta, OpenAI, and Anthropic to use copyrighted work without the copyright owner’s permission under some circumstances. These resources are then used to train AI. The authors in the Meta case sued in 2023, alleging that the company used pirated versions of their books to train Llama without permission or compensation.

In response, technology companies stated that the obligation to pay copyright holders for their content could hamstring the burgeoning AI systems.

While the plaintiffs claimed that AI companies unlawfully copied their work to generate competing content that threatened their livelihoods, the defendants argued that their AI systems made fair use of copyrighted material by studying it to learn to create transformative content.

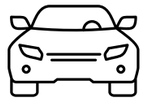
European Commission Releases Report on Competition Policy 2024

The European Commission published its Report on Competition Policy 2024 on its official website for competition activities.

The Report covers modernization and simplification of competition rules, green transition and digital transformation, effective implementation of the Digital Markets Act (DMA) and the Foreign Subsidies Regulation (FSR), and the effects of competition policies and practices.

In addition to regulatory updates, the Report also outlines developments in 2024 regarding competition investigations, M&A investigations, state aid measures and Important Projects of Common European Interest (IPCEI).

2024 was a busy year in terms of M&A investigations, along with significant decisions on Mondelez, Vifor Pharma, Teva Copaxone, Apple App Store, Apple Pay and Meta Facebook Marketplace in competition investigations. In 398 investigations, 8 transactions were allowed with commitments, while others were allowed directly. In 2024, 127 state aid measures were also granted. In addition to developments regarding the DMA and FSR regulations, the European Commission Competitiveness Compass was also published at the beginning of 2025 based on activities in 2024.



Tesla Sued in the US for Allegedly Speeding up Odometers to Avoid Warranty Repairs

Tesla faces a lawsuit for allegedly speeding up odometers on its electric vehicles so that they fall out of warranty faster, thus saving the company from having to pay for repairs.

The plaintiff Nyree Hinton alleged that Tesla odometer readings reflected energy consumption, driver behavior and “predictive algorithms” rather than actual mileage driven. Tesla took the case to Los Angeles state court.

Although Tesla and its lawyer did not immediately respond to requests for comment, they denied all material allegations in the lawsuit. Compensation was demanded for Tesla drivers in California, potentially encompassing more than 1 million vehicles, as shown by court papers.

Tesla also faces actions accusing it of inflating vehicle driving ranges. In March 2024, a federal judge in Oakland, California, said that drivers in that case should pursue their claims in individual arbitrations, not a class action.

The case is Hinton v Tesla Inc et al, U.S. District Court, Central District of California, No. 25-02877.

Tension Escalates Between Law Firms and the US Administration

On April 11 in Washington, a new case was brought before the judiciary challenging executive orders issued by US President Donald Trump against several prominent law firms. The law firm Susman Godfrey sued the Trump administration due to an executive order that it said violated its constitutional rights. This is the fourth lawsuit filed against Trump’s sanctions. The petition warned that the executive order crossed constitutional boundaries and set an example for future presidents to target their political enemies. The firm claimed that Trump’s executive order was a form of political revenge for the firm’s representation of Dominion Voting Systems regarding the 2020 elections.

Lawyers at the law firms targeted by Trump’s executive orders have been restricted from accessing government agencies, and their clients’ federal contracts are at risk. The proposed justification for these measures was that these firms were associated with people and lawsuits that Trump opposed.

On the same day, Trump announced that five major law firms reached an agreement with the administration due to pressure. As such, these firms agreed to provide free legal services worth more than $600 million in social projects supported by Trump. Thus, the amount of pro bono work committed to Trump by law firms reached $940 million in the last month. Each of the firms that reached an agreement will offer support to the projects selected by Trump and abandon their diversity-based employment practices. With these agreements, the US Equal Employment Opportunity Commission has also halted investigations into the employment practices of the relevant firms.

While the companies did not comment publicly, their internal correspondence was leaked to the press. Simpson Thacher Chairman Alden Millard and Kirkland & Ellis management stated that the agreements would not undermine the control of the companies and that the decisions were made for strategic reasons. During Trump’s first presidential term, many of these firms had filed lawsuits against the administration’s policies on various issues, including immigration, voting rights and gender identity. Trump said the companies now provided legal services for him and could also be involved in future trade deals.

News from Şengün

Legality / News from Şengün

Legality
News from Şengün

///

Şengün & Partners Attorney Partnership released an article titled “Türk Şirketleri İçin Alman Tedarik Zinciri Yasası ve AB Tüzüğü Riskleri” (i.e. Risks of German Supply Chain Act and EU Regulation for Turkish Companies), written by Founding Partner Nedim Korhan Şengün, Partner Gülşah GÜVEN, LL.M., and Partner Birgi Kuzumoğlu, as part of its Şengün Law publications.

///

Şengün & Partners Attorney Partnership announced its gig initiative “BAĞLANTI”. Welcoming gig lawyers for local and global cooperation to create shared value, the initiative attracted strong interest following its launch.

Legality / News from Şengün

Legality
News from Şengün

Şengün & Partners Attorney Partnership launched its “PLATFORM” project, a new digital consultancy model. Through PLATFORM, users can fill out a form and schedule an appointment to receive legal advice from experienced attorneys. Conversations will be completely confidential and secure.

Şengün & Partners Competition Law Institute published the first issue of its special newsletter covering competition law updates in Türkiye and worldwide.

The Board of Directors of Şengün & Partners Attorney Partnership held a meeting, taking decisions on the working principles of the Attorney Group and Şengün & Partners Competition Law Institute (“Institute”).

At the meeting, the Board decided to intervene in and fight against the risks posed by digital monopolies on the rule of law, democracy and human rights to support harmony within a democratic system. The meeting started with a speech by President Nedim Korhan Şengün and continued with a presentation by Vice President Dila Yıldırım. Following the presentation that discussed the risks of digital monopolies for the rule of law, democracy and human rights, the participants identified solutions and strategies to prevent digital monopolization.

The relevant press release contained the following statements: “We will stand for justice and an open and transparent market against all forms of monopolization, especially digital monopolies. Working for the rule of law, the individual’s right to choose and democratic control mechanisms is not only a professional choice but also a duty.”

It was also announced that a thorough approach would be adopted to address the issue, with regular public updates and all necessary legal procedures.

Legality
News from Şengün

Şengün Global, which offers a global perspective by combining local expertise with international standards, released a newsletter titled “Crypto Asset Regulations in Türkiye: An Overview of Developments in the Last Five Years”, written by Associate İdil Aşkın under the guidance of Partner Gülşah GÜVEN, LL.M.

Şengün & Partners Sustainability and Compliance Center (SUM) published its first Special Newsletter for 2025, prepared by Associate Selin Ünverdi and other relevant associates under the guidance of Partner Birgi Kuzumoğlu, as part of its efforts to support companies in developing sustainable policies on environmental, social and governance (ESG) issues.

Legality / News from Şengün

Şengün Academy released a newsletter titled “Türkiye’de Kripto Düzenlemeleri: Beş Yıl İçinde Yaşanan Gelişmelere Genel Bakış” (i.e. Crypto Asset Regulations in Türkiye: An Overview of Developments in the Last Five Years), written by Associate İdil Aşkın under the guidance of Partner Gülşah GÜVEN, LL.M.

Şengün & Partners Industrial Law Center presented a newsletter titled “Labor Law Considerations in Mergers and Acquisitions”, written by Executive Associate Öykü Güldürmez and Associate Selin Ünverdi under the guidance of Senior Associate Betül Önal Payze.

Legality
News from Şengün

Şengün & Partners Attorney Partnership and Şengün & Partners Competition Law Institute held a webinar titled “Rekabet Kurumu Soruşturmalarında Sözlü Savunma Teknikleri” (i.e. Oral Hearing Strategies in Competition Investigations) on 28 April 2025 at 16:00.

Associate İdil Aşkın at Şengün & Partners Attorney Partnership presented the webinar and explained the basic rules in oral hearings, a significant stage in the Competition Authority investigations. The webinar provided examples from recent oral hearings, analyzing the latest developments in competition law and focusing on common characteristics observed during hearings.

Offering practical information as well as a theoretical framework on competition law, the webinar united company professionals and interested parties upon special request.

Şengün & Partners Investment & Capital Markets released a special newsletter, written by Associate Ahmet Oğul Aksoy and Legal Intern Meryem Torkay under the guidance of Executive Associate Yiğit Okuldaş.

Sales Network held its HR Summit at UNIQ Istanbul on May 8, 2025, uniting the leading names of the sales and human resources ecosystem. The event was opened with a speech by Sales Network Founder Ergün Güler and focused on the concepts of artificial intelligence, human and trust. Upon invitation, Şengün & Partners Attorney Partnership participated in the event, represented by Founding Partner Nedim Korhan Şengün and Associate Dila Yıldırım.

Legality / News from Şengün

Legality
News from Şengün

Şengün & Partners Competition Law Institute released its second newsletter covering competition law updates in Türkiye and worldwide.

Founding Partner Nedim Korhan Şengün at Şengün & Partners Attorney Partnership held a meeting with strategic business partners, external consultants (legal consultants and specialists) academics, legal tech experts, corporate communication specialists, and lawyers serving as of counsel. At the meeting, participants discussed a variety of subjects, including progress toward the goals established at the 2021 General Assembly of Şengün & Partners Attorney Partnership, developments regarding the relevant companies, the academy, and the institute, as well as global updates in the legal industry, and institutional transformation. The meeting ended with a speech by Founding Partner Nedim Korhan Şengün, who emphasized the ongoing transformations in the legal profession.

The conference titled “Recent Developments in Geographical Indications in Türkiye and the EU”, organized by the Turkish Patent and Trademark Office (TÜRKPATENT), was held with the participation of M. Zeki Durak, President of the Turkish Patent and Trademark Office, João Onofre, Head of the Geographical Indications Unit at the Directorate-General for Agriculture and Rural Development of the European Commission, Hasan Çağlayan Dündar, Advisor to the President of TOBB, Cahit Ceren, Director of SME Policies at TOBB, and Aslı Parmak, Legal Expert in SME Policies at TOBB.

Upon invitation, Associate Ahmet Oğul Aksoy and Legal Intern Meryem Torkay attended the conference on behalf of Şengün & Partners Attorney Partnership on May 13, 2025. The conference addressed topics such as the management of geographical indications, regulations, sustainability, Türkiye’s significance in the field of geographical indications, effective monitoring, and branding processes. Evaluations were shared with stakeholders during networking breaks and in one-on-one discussions.

Legality / News from Şengün

Legality
News from Şengün

Our Associate Dila Yıldırım attended the Career Day event organized by the high school she graduated from, i.e. İstek Semiha Şakir Anatolian High School, upon the school's kind invitation.

At the event, she candidly shared her experience and offered insights into the legal profession, touching on significant topics such as legal education, professional development, and business life.

On May 14, 2025, our Founder Nedim Korhan Şengün and Senior Associate Betül Önal Payze hosted a visit from Karabulut & Arkat Attorney Partnership, including Founding Partner Özgür Karabulut, Partner Hacer İlhan Arkat, and student interns Almina Meydeş, Efe Kutay Alaçiçek, and Mehmet Alp İlhan.

During the friendly meeting, the participants exchanged views on recent legal developments, shared professional experiences, and offered diverse perspectives.

The participants also spoke about İzmir's position in the business and legal landscape.

Şengün & Partners National and EU Registration Consulting Center for Geographical Indications released its "Geographical Indications Newsletter" prepared under the guidance of our Founder Nedim Korhan Şengün and Partner Birgi Kuzumoğlu.

Legality
Sources

- https://www.resmigazete.gov.tr/eskiler/2025/03/20250330-1.htm
- https://www.resmigazete.gov.tr/eskiler/2025/03/20250308-1.htm
- https://resmigazete.gov.tr/eskiler/2024/10/20241030-2.htm

Legality
Location

Legality

"A seminal publication of Şengün Group"

April - May 2025 | E-Bulletin