

# THE FINE PRINT

Answers. Not theories.

**2025**

## AMENDMENTS TO TURKISH DATA PROTECTION LEGISLATION: CROSS-BORDER DATA TRANSFERS

- The Golden Year of Crypto Regulation in Turkey
- The Advertising Board Keeps a Close Eye on the Digital World, Tackles Dark Patterns
- Turkish Competition Authority Continues to Scrutinize Technology Giants: Meta and Google
- A Year of Cybersecurity: A Brief Overview of International and National Developments
- An Era Has Closed: Article 9 of Internet Law No. 5651 Repealed

# “FROM THE EDITOR,”

As we reach the end of a long year, we reflect on the exciting developments we experienced as Gökçe Attorney Partnership, as announced in June. With our strengthened team and new office, we continue to deliver our services more efficiently and effectively. Our modern work environment and advanced technological infrastructure have enhanced our team's productivity and enabled us to meet our clients' expectations at the highest level. Our efforts to strengthen international collaborations remain steadfast, as we move forward with innovative solutions and a solid foundation.

We wish all our friends, clients, and business partners a 2025 filled with health, success, happiness, and prosperity. Here's to achieving even greater accomplishments together!

*Görkem Gökçe*

## Amendments to Turkish Data Protection Legislation: Cross-Border Data Transfers

The year 2024 marked a turning point in Turkey's Personal Data Protection Law (KVKK), particularly concerning the long-awaited reforms in cross-border data transfers. Since its inception, KVKK has sparked numerous debates, with frequent criticism about the inadequacy of its cross-border data transfer provisions to address modern requirements. These criticisms paved the way for ongoing reform efforts within KVKK.

On March 12, 2024, the Eighth Judicial Package came into effect, introducing critical amendments to KVKK, particularly on cross-border data transfers and the processing of sensitive personal data. With these changes, the cross-border data transfer framework underwent a significant overhaul, adopting a structure more aligned with GDPR. A three-tiered and alternative-based transfer regime was established for transferring personal data abroad under KVKK:

- Transfers based on adequacy decisions,
- Transfers based on appropriate safeguards,
- Transfers based on exceptional circumstances.

The inclusion of "binding corporate rules" (BCRs) and "standard contractual clauses" (SCCs) under the appropriate safeguards framework addressed longstanding concerns and alleviated some of the complexities surrounding cross-border data transfers. However, debates about the methods and scope of implementation persisted for a significant period.

### Regulation on Cross-Border Data Transfers

Secondary legislation concerning KVKK's amendments was introduced on July 10, 2024, through the Regulation on Procedures and Principles Regarding Cross-Border Data Transfers. This Regulation resolved many ambiguities, particularly around SCCs, and shed light on key aspects of implementation.

The Regulation detailed the scope of SCCs and outlined the notification processes to the Personal Data Protection Authority (KVKK Authority). It also provided clarity on application procedures for binding corporate rules. Furthermore, the KVKK Authority published sample SCCs and BCR documents on its official website, making them readily available for practical use.

For a detailed analysis of the KVKK amendments and the regulation, please refer to our [TFP Special Issue](#), as well as the [TFP May](#) and [TFP July](#) issues.

### Standard Contract Notification Module: Simplifying Implementation

One of the questions that arose from the new framework was the obligation to notify the KVKK Authority about the use of SCCs. This requirement drew attention, particularly since no equivalent obligation exists under GDPR, raising curiosity about how the Authority would address this matter.

To address these concerns, the KVKK Authority introduced the Standard Contract Notification Module on October 25, 2024. This online platform aims to simplify the process of submitting SCC notifications, eliminating the operational challenges associated with physical submissions. The module was launched alongside a comprehensive guide. For further details, refer to our [TFP November](#) issue.

The reforms introduced in 2024, and the subsequent developments reflect a concerted effort to make KVKK more effective and internationally aligned. While GDPR compliance remains a key objective for Turkey, these changes signify a major shift in practice, hinting at further advancements in the coming years. We eagerly await additional amendments and updates to the legislation.

## The Golden Year of Crypto Regulation in Turkey

2024 was an intense year for cryptocurrency regulations in Turkey. As we comprehensively covered in our [July TFP issue](#), the amendments known publicly as the "Crypto Asset Law" were enacted as part of the Law Proposal on Amending the Capital Markets Law and published in the Official Gazette on July 2, 2024. This regulation established a broad framework, including defining crypto asset service providers (CSPs) and platforms, their obligations, and their supervision.

### A Brief Recap: July 2024 Regulations

- **Powers of the CMB:** The Capital Markets Board (CMB) gained the authority to determine the principles for crypto asset issuance and regulate the contractual provisions concerning service providers and platforms.
- **Obligations for CSPs and Platforms:** New obligations were introduced, such as establishing an internal control unit, undergoing independent audits, and segregating users' assets.
- **Sanctions:** Severe administrative and criminal penalties were introduced for unauthorized activities.

### New Developments

Following the enactment of the Crypto Asset Law, several steps were taken to further regulate the sector throughout the rest of the year:

- **Publication of Lists:** In accordance with Provisional Article 11 of the Capital Markets Law, lists were published to inform the public about entities declaring their intention to operate. These included: (i) [The List of Entities in Operation](#), (ii) [The List of Entities Declaring Liquidation](#), (iii) [The List of Platforms Whose Applications Were Rejected](#), (iv) [The List of Platforms Whose Applications Were Not Processed](#) (Only available in Turkish).
- **TUBITAK's Role:** Under the Crypto Asset Law, TUBITAK's role in the licensing processes of CSPs became clearer. TUBITAK undertook responsibilities such as:
  - Determining technical criteria CSPs must meet
  - Preparing technical reports on the originality of blockchain projects
  - Participating in audits
  - TUBITAK's ongoing efforts are eagerly awaited.
- **Secondary Regulations:** On December 25, 2024, changes published in the Official Gazette ushered in a new era in combating money laundering, countering terrorist financing, and fighting the informal economy. Key regulations affecting CSPs include:
  - **Regulation on Measures to Prevent Money Laundering and Terrorist Financing:** CSPs were included within the scope of financial institutions under MASAK regulations. Messages regarding crypto asset transfers of

TRY 15,000 or more must include: Sender's full name, trade registry title (for legal entities), or full legal entity name, wallet address or transaction reference number, at least one identifier for the sender. These details must be verified. The same applies to recipient details, although verification is not mandatory. Transfers to or from unregistered wallet addresses must include a declaration from the client confirming at least one identifier. These regulations take effect on February 25, 2025. You can access the regulation on the relevant amendments [here](#) (Only available in Turkish).

- **Regulation on MASAK Electronic Notification System Procedures:** Notifications from MASAK under the Law on the Prevention of Financing Terrorism can now be made to CSPs electronically. Entities declared active by the CMB must apply to MASAK for account creation within a month of December 25, 2024. You can access the regulation on the relevant amendments [here](#). (Only available in Turkish).
- **Regulation on Compliance Programs for Obligations to Prevent Money Laundering and Terrorist Financing:** CSPs were added to the list of entities required to establish compliance programs under MASAK regulations. These programs aim to prevent money laundering and terrorist financing. You can access the regulation on the relevant amendments [here](#). (Only available in Turkish).
- **MASAK General Communiqué No. 19:** Stricter measures were introduced for remote identity verification. CSPs facilitating the trading or storage of privacy-focused crypto assets can no longer perform remote identity verification. Additionally, for establishing continuous business relationships, all financial transactions, including deposits and withdrawals, must be conducted through bank or credit card accounts matching the customer's verified identity information. You can access the regulation on the relevant amendments [here](#). (Only available in Turkish).

2024 marked a significant starting point for the regulation of the cryptocurrency ecosystem in Turkey. With the completion of secondary regulations and the clarification of practices, the sector is expected to achieve greater stability and security in 2025.

## The Advertising Board Keeps a Close Eye on the Digital World, Tackles Dark Patterns

The rapid advancements in digitalization have not only increased consumers' reliance on online platforms but have also exposed them to a greater volume of digital advertisements and applications. This "digital consumer" group, whose rights are highly vulnerable and whose data is becoming increasingly valuable, was the focal point of the Advertising Board's efforts throughout the year. With a significant portion of its decisions in 2023 focused on digital advertisements, the Board continued this approach in 2024.

In particular, the Advertising Board stood out for its initiatives aimed at preventing consumer manipulation, making significant strides toward compliance with both national and international standards. Here are some highlights from 2024:

### Combatting Dark Patterns

In 2024, the Advertising Board reinforced its commitment to protecting digital consumer rights by intensifying its fight against dark patterns. These are deceptive digital strategies that restrict consumers' decision-making freedom, steering them

in favor of businesses. The concept was first rigorously addressed in a 2022 OECD report titled *"Dark Commercial Patterns"* and has since remained a central focus in consumer protection discussions.

Evaluating the unethical nature of these patterns, the Board made significant decisions targeting methods that lead consumers to make unconscious or manipulated choices. The October 2024 meeting focused extensively on dark patterns, with the Board solidifying its stance through precedent-setting decisions. Key findings included:

- Requiring mandatory payment information for "free trial" services,
- Misleading designs involving colors, sizes, or navigational cues,
- Subscription agreements that pressure users into giving consent,
- Notifications such as "...added this to their favorites" or "...items in someone's cart," which adversely influence consumer decision-making,
- Using more attention-grabbing colors for buttons directing consumers toward specific actions.

### Personal Data Misuse and Targeted Advertising

The misuse of personal data and processes for targeted advertising were also key issues on the Board's agenda. To prevent data exploitation, the Board emphasized the following points through its decisions:

- Processing personal data for targeted advertising without explicit consent,
- Forcing consumers to accept cookie preferences without adequate information,
- Restricting users' ability to manage their data during membership or subscription processes.

To address these issues, the Board signed a collaboration protocol with the Personal Data Protection Authority. This partnership aimed to enhance data security and ethical commercial practices. When announcing the protocol, the institutions highlighted the risks associated with the excessive use of personal data in targeted advertising and dark patterns. They stressed that these practices not only violate personal data privacy but also influence consumers' purchasing behaviors. The joint statement emphasized the importance of increasing consumer awareness and strengthening control over their personal data at the intersection of personal data law and consumer law.

The Advertising Board's proactive role in consumer protection policies, its fight against dark patterns, and its heightened sensitivity to data-driven commercial activities aim to create a fairer and more transparent digital landscape.

These steps are critical not only for addressing today's challenges but also for serving as a guide to protect digital consumer rights in the future. For more insights on this topic, refer to the [April](#), [June](#), [September](#), and [October](#) issues of the TFP Bulletin.

## Turkish Competition Authority Continues to Scrutinize Technology Giants: Meta and Google

In 2024, the Turkish Competition Authority maintained its focus on global technology giants, particularly Meta and Google, closely monitoring and evaluating their practices. Given the significant market share these companies command through their products and services, nearly every aspect of their operations holds relevance from a competition law perspective. To ensure fair competition in the digital market, the Authority conducted investigations into specific practices and behaviors of these corporations. Some key cases are outlined below.

### Investigations into Google

#### Search Results and Market Dominance

The Competition Board investigated whether Google's general search results page, through specific search features, disadvantaged other websites by "pushing them down" and causing a loss of traffic. The primary focus of this inquiry was whether Google abused its dominant position. The Board concluded that Google had not abused its dominance and decided not to impose an administrative fine.

#### Local Search and Hotel Ads

One of the most notable investigations of the year involved Google's practices concerning local search (Local Unit) and hotel price comparison (Google Hotel Ads - GHA) services. The Board examined whether Google had positioned its Local Unit and GHA services more advantageously on general search results pages, thereby excluding competitors. The investigation found abuse of dominance, leading to a fine of approximately 482 million Turkish Lira. The Board also issued compliance recommendations to Google and provided a deadline for implementation.

#### Online Advertising Technology

In December 2024, the Board concluded another investigation into Google's practices in online display advertising and ad technology services. The allegations included claims that Google directed inventory purchase requests from its demand-side platforms (DSPs) to its own supply-side platforms (SSPs) and favored its SSP service (AdX) through its publisher ad server. Additionally, concerns were raised about restricting the purchase of YouTube inventory exclusively through Google's DSPs.

The Board found no violation regarding DSP-to-SSP redirection but determined that Google had unfairly advantaged its SSP service and engaged in self-preferencing, which hindered competitors' activities. Consequently, the Board imposed a fine of approximately 2.6 billion Turkish Lira and outlined the conditions that needed to be rectified.

The full text of the relevant decision announcement is available [here](#) (Only available in Turkish). For details of the decisions, you can refer to [TFP June](#) and [TFP July](#) issue.

#### Investigation into Meta and Threads

The Board launched an investigation into Meta over allegations that it linked its Threads application to Instagram, merging user data in violation of Article

6 of the Competition Law. In February, the Board issued interim measures and imposed a daily administrative fine of approximately 4.8 million Turkish Lira until compliance was achieved.

In response, Meta proposed solutions, such as introducing "profile-free use" features similar to those implemented for EU users. However, the Board deemed these measures insufficient. Subsequently, Meta deactivated all Threads user profiles in Turkey.

In a final move, Meta submitted a commitment on October 30, 2024, stating that Threads users in Turkey would be able to access the app exclusively through a Threads profile without requiring an Instagram account. Meta also pledged that data collected through Threads would not be shared with Instagram unless accounts were merged. The Board accepted this commitment, concluding the investigation.

These developments underscore the Turkish Competition Authority's vigilance in regulating dominant market players and ensuring fair competition in the digital economy. With its proactive stance, the Authority continues to set a precedent for addressing challenges in the fast-evolving digital landscape.

The full text of the relevant decision announcement is available [here](#) (Only available in Turkish).

## A Year of Cybersecurity: A Brief Overview of International and National Developments

### The EU Cyber Resilience Act (CRA)

One of the most significant and exciting developments in cybersecurity was the introduction of the Cyber Resilience Act (CRA), published in November 2024. The Act establishes cybersecurity standards for digital products across the European Union. It places obligations on manufacturers to ensure security throughout a product's lifecycle and extends its scope to software developers, importers, and distributors.

The CRA covers a wide range of products, from Internet of Things (IoT) devices to high-risk artificial intelligence systems. It mandates manufacturers to regularly test their products for vulnerabilities and address any issues promptly. To enhance its deterrent effect, the Act imposes substantial fines for security breaches, reaching up to €15 million. Although most provisions of the CRA will be enforceable from December 11, 2027, some are set to take effect earlier.

Details are in our [TFP November](#) issue.

### The UN Cybercrime Treaty Draft

On August 9, 2024, the United Nations achieved a milestone by publishing the draft of a treaty aimed at strengthening the global fight against cybercrime. This draft encourages member states to work collectively in areas such as freezing and confiscating proceeds of cybercrimes, collecting and sharing electronic evidence, and harmonizing national laws.

The treaty covers a wide range of offenses, including data breaches, computer-related crimes, and money laundering. It also includes an action plan to provide member states with an effective framework for investigating cybercrimes

and accelerating international cooperation on electronic evidence sharing. If approved by the UN General Assembly, this draft will become the first of its kind.

For more details, have a look at our [TFP August](#) Bulletin.

#### **Turkey's National Cybersecurity Strategy and Action Plan (2024–2028)**

Led by the Ministry of Transport and Infrastructure, Turkey's National Cybersecurity Strategy and Action Plan aims to enhance the country's cybersecurity capacity, addressing emerging technologies like 5G, IoT, and big data analytics. Developed under the principles of "zero trust" and "security by design", the plan emphasizes domestic and national solutions to counter cyber threats.

The strategy outlines six key objectives, including:

- Enhancing cyber resilience
- Implementing proactive cyber defense measures
- Strengthening deterrence
- Promoting Turkey's international cybersecurity brand

Additionally, the plan features comprehensive actions to instill a cybersecurity culture within organizations, encourage local research and development, and adopt a holistic approach to combating cyber threats.

These developments collectively reflect a significant year for cybersecurity, with critical steps taken both globally and nationally to address evolving threats in the digital age.

For a detailed examination of the topic, you can access [TFP September](#) issue.

## **An Era Has Closed: Article 9 of Internet Law No. 5651 Repealed**

With the Constitutional Court's decision published in the Official Gazette on 10 January 2024, certain provisions of Internet Law No. 5651, which had been a topic of discussion for a long time, were annulled as unconstitutional. Following this decision, the repeal of the relevant provisions came into effect on 10 October 2024.

In 2020, amendments to Article 8 of Internet Law No. 5651 granted the Information and Communication Technologies Authority (ICTA) the authority to issue ex officio decisions regarding the removal of content and blocking access to content related to specific catalog crimes. Additionally, administrative sanctions were introduced for content, hosting, and access providers that failed to comply with ICTA decisions.

However, the Constitutional Court determined that these provisions violated the presumption of innocence and deemed it unlawful for administrative authorities to make decisions on acts classified as crimes under criminal law. As a result, these provisions were annulled.

Article 9, which addressed content removal and access blocking in cases of personal rights violations, was also repealed. The Constitutional Court argued that this article could cause significant interference with freedom of expression and press freedom, imposing a disproportionate restriction. The court concluded that the article failed to offer more gradual and balanced measures to protect personal rights, leading to its annulment.

In conclusion, it can be said that an era came to an end as of 10 October 2024.

Details on the Constitutional Court's decision are in our [TFP January](#) issue.

## Editors



**Görkem Gökçe**

[gorkem.gokce@gokce.av.tr](mailto:gorkem.gokce@gokce.av.tr)



**Dr. Mehmet Bedii Kaya**

[bedii.kaya@gokce.av.tr](mailto:bedii.kaya@gokce.av.tr)



**Elif Aksöz**

[elif.aksoz@gokce.av.tr](mailto:elif.aksoz@gokce.av.tr)



**Yağmur Yollu**

[yagmur.yollu@gokce.av.tr](mailto: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](http://www.gokce.av.tr) for further information on our legal staff and expertise.

**Please contact us at**  
[info@gokce.av.tr](mailto:info@gokce.av.tr)  
0 212 352 88 33

The Fine Print is prepared and published for general informative purposes only and does not constitute legal advice or create an attorney-client relationship. Should you wish to receive further information, please contact Gokce Attorney Partnership. No content provided in The Fine Print can be reproduced or re-published without proper attribution or the express written permission of Gokce Attorney Partnership. While all efforts have been made to ensure the accuracy of the content, Gokce Attorney Partnership does not guarantee such accuracy and cannot be held liable for any errors in or reliance upon this information. The Fine Print was created for clients of Gokce Attorney Partnership and the possibility of circulation beyond the firm's clientele should not be construed as advertisement.