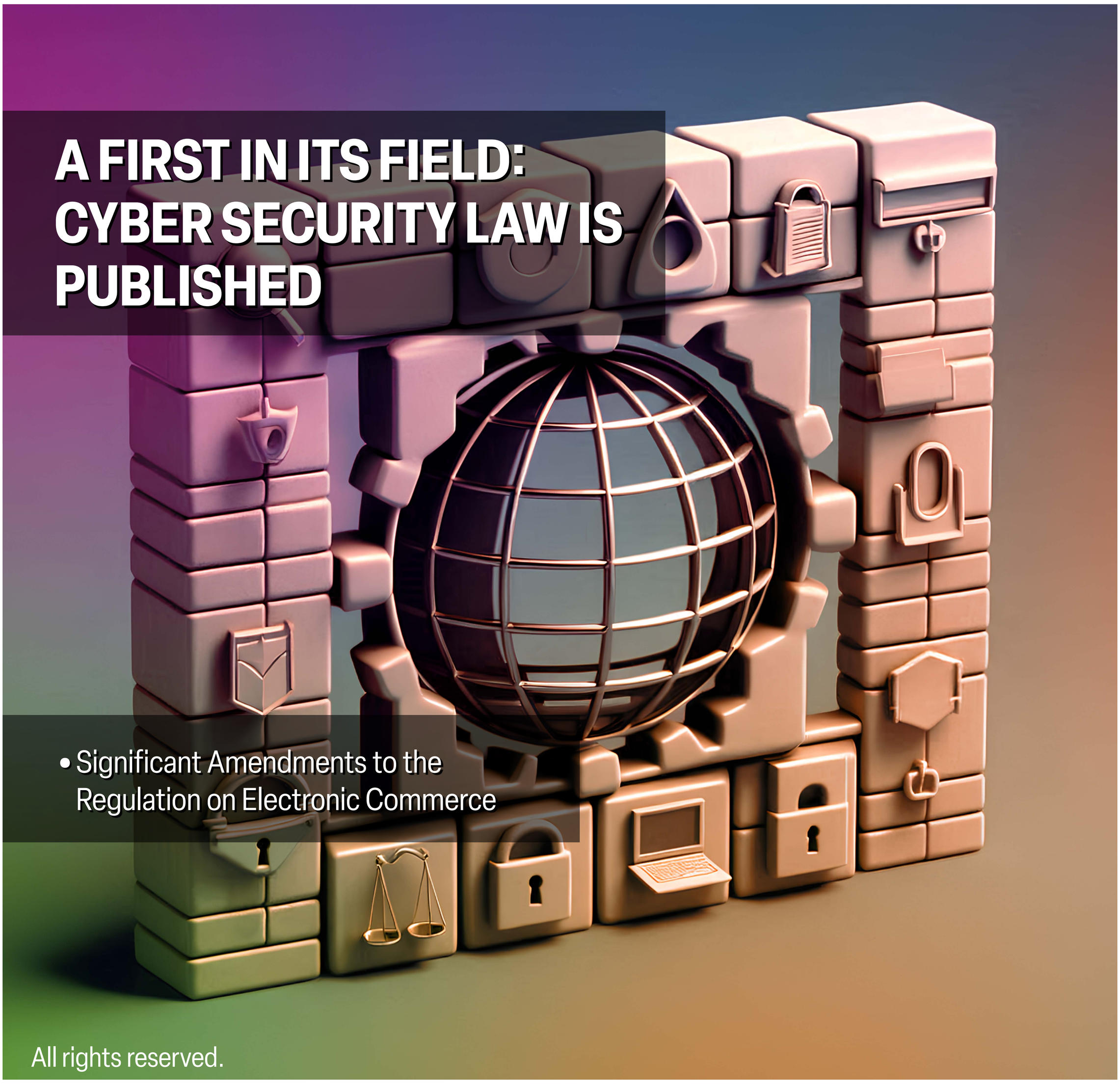
MARCH 2025 Gökçe ISSUE: 136

# THE FINE PRINT

Answers. Not theories.



## A FIRST IN ITS FIELD: CYBER SECURITY LAW IS PUBLISHED

- Significant Amendments to the Regulation on Electronic Commerce

# A First in its Field: Cyber Security Law is Published

Turkey is facing a striking regulation in the field of cybersecurity: The Cyber Security Law **(Law)** was published in the Official Gazette on 19 March 2025.

Until now, there was no comprehensive framework legislation regulating the field of cyber security under Turkish law. With the Law, a significant gap has been fulfilled.

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

The Law covers all public institutions and organisations, professional associations, real and legal persons operating in cyberspace.

The activities carried out by the National Intelligence Organisation and the activities of the General Directorate of Security and the Gendarmerie General Command, as well as the activities carried out in accordance with the Law on State Intelligence Services and the National Intelligence Organization and the Law on Internal Service of the Turkish Armed Forces are excluded from the scope of the Law.

The outstanding regulations in the Law are as follows:

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

Significant definitions and novelties brought with the Law are as follows:

The Cyber Security Presidency **(Presidency)** assumes a proactive role against cyber threats. This role includes vital responsibilities such as increasing the cyber resilience of critical infrastructures, detecting, preventing and mitigating cyber-attacks.

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

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

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

Although not included in the definitions section, the Cyber Security Board was also established under the Law. The purpose of the Board is to take decisions on policies, strategies, action plans and other regulatory actions related to cyber security and to determine the institutions and organisations that will be exempted from all or some of the decisions taken.

**The main duties and responsibilities regarding cyber security of those who provide services, collect, process data and carry out similar activities by using information systems:**

- Transmit all kinds of data, information, documents, hardware, software and any other contribution requested by the Presidency within the scope of its duties and activities to the Presidency primarily and on time. This point is quite critical. Because violation of this regulation brings imprisonment and administrative fines.
- To take the measures stipulated by the legislation for the purposes of national security, public order or the proper execution of public service regarding cyber security, and to report the vulnerabilities or cyber incidents detected in the area where the service is provided to the Presidency without delay.
- To procure cyber security products, systems and services to be used in public institutions and organisations and critical infrastructures from cyber security experts, producersor companies authorised and certified by the Presidency.
- Cyber security companies subject to certification, authorisation and certification must obtain the approval of the Presidency before commencing operations.

**The criminal sanctions in the Law:**

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

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

- Those who create misleading content regarding data leaks in cybersecurity, or disseminate such content for this purpose, in order to create anxiety, fear and panic among the public or to target institutions or individuals, despite being aware that there is no data leak in cyberspace, will be sentenced to **imprisonment from two to five years**. The relevant regulation has caused widespread resonance within the public opinion. This is mainly the case due to the broad interpretation of the article. This part of the Law should be interpreted in a way that does not prejudice freedom of expression.

The sale abroad of cyber security products, systems, software, hardware and services and the merger, division, share transfer or sale transactions of the companies producing them will be subject to the approval of the Presidency. Any actions taken in the absence of presidential approval will be unlawful.

Although the Law will enter into force on its date of publication, companies operating in the field of cyber security are obliged to complete their certification processes within one year from the entry into force of the relevant regulations.

Secondary regulations are expected to be completed within one year.

Cybersecurity has taken its place at the top of the agenda as a new compliance requirement for everyone. New developments are eagerly awaited.

You can access the Law here. *(Only avaliable in Turkish)*.

## Significant Amendments to the Regulation on Electronic Commerce Intermediary Service Providers and Electronic Commerce Service Providers

Important amendments have been introduced to the Regulation on Electronic Commerce Intermediary Service Providers and Electronic Commerce Service Providers **(Regulation)** through two separate regulations published in the Official Gazette on 8 March 2025 and 15 March 2025.

Among these, the regulation published on 8 March 2025, which entered into force on the same date, introduces more critical provisions. With this amendment, several new rules have been enacted, ranging from the relationship between electronic commerce intermediary service providers **(ECISPs)** and electronic commerce service providers **(ECSPs)** to the calculation of e-commerce licensing fees. Key changes include:

- ECSPs operating on e-commerce marketplaces are now obliged to notify the ECISP of various details concerning their activities.

- ECISPs may impose contractual penalties on ECSPs without requesting an explanation, provided that the conditions giving rise to the penalty (as stipulated in the intermediary agreement) can be substantiated. Any deviation from this rule shall be deemed an unfair commercial practice.

- Information within the internal communication system, which could previously only be accessed by personnel assigned by the Ministry of Trade, can now be viewed, recorded, and copied without modification by ECSPs during the term of the intermediary agreement and for one year following its termination.

- Following the termination of an intermediary agreement, medium, large, and very large-scale ECISPs are now required to enable ECSPs to transfer the specified data listed under the Regulation for a period of one year. Previously, this obligation ceased upon termination of the agreement.

- As is known, ECISPs and ECSPs were prohibited from advertising using the registered trademarks of unrelated third parties as keywords in online search engines. While the Ministry of Trade previously notified the parties in case of violation, it is now authorized to directly impose administrative sanctions. Furthermore, in the event of such infringement, ECISPs and ECSPs must not only cease the violation but also include the relevant keywords in their negative keyword list and provide proof thereof to the Ministry.

The amendments also include substantial changes to the calculation of the electronic commerce licensing fee. Noteworthy updates are as follows:

- Sales made abroad via e-commerce marketplaces by ECISPs and affiliated entities within the same economic entity will not be taken into account in the licensing fee calculation.

- The concept of “foreign sales” has been broadened. In addition to direct orders, sales of goods shipped abroad prior to orders, as well as transactions conducted using foreign IP addresses or foreign credit cards, will also be considered foreign sales.

- If the net transaction volume of an ECISP does not exceed 20% of the total net transaction volume of ECISPs and ECSPs (as calculated based on ETBIS data), then, for the following calendar year, the amount of foreign sales and twice the amount of investment expenditures made under an investment incentive certificate issued by the Ministry of Industry and Technology will be deducted from the net transaction volume of that year. However, in determining whether this 20% threshold has been exceeded, any excess below 15% will be disregarded.

- The value of foreign sales, excluding cancellations and returns, will be calculated based on final invoices or equivalent documents issued by ECISPs, their affiliated entities, and ECSPs selling via e-commerce marketplaces.

- The burden of proof regarding transactions declared as foreign sales lies with the declaring ECISP.

The legislative framework governing electronic commerce has undergone substantial revisions, particularly through secondary legislation. These latest amendments are of significant importance for all actors in the sector.

You may access the relevant amending regulations here and here. *(Only avaliable in Turkish)*.

## Editors


**Görkem Gökçe**
gorkem.gokce@gokce.av.tr

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

**Elif Aksöz**
elif.aksoz@gokce.av.tr

**Yağmur Yollu**
yagmur.yollu@gokce.av.tr


## About us

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


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