



LATEST NEWS

- A bill containing artificial intelligence regulations has been submitted to the Turkish Grand National Assembly.
- Istanbul Governorate's decision regarding 24-hour continuous video and audio recording.
- A proposed amendment to the Internet Law No. 5651 has been submitted to the Turkish Grand National Assembly.
- A bill on the ratification of the "Digital Economy Partnership Agreement between the Governments of Member States of the Organization of Turkish States" was submitted to the Grand National Assembly of Turkey.
- Special recommendations from KVKK for November 30 Computer Security Day.
- The Personal Data Protection Authority has published the "Guide on Generative Artificial Intelligence and the Protection of Personal Data (15 Questions)."

GLOBAL NEWS

- UNICEF has released a new report on protecting children in online games.
- The European Commission has published a document titled "Data Union Strategy – Unlocking Data for Artificial Intelligence."

ARTIFICIAL INTELLIGENCE TECHNOLOGIES AND THE NEED FOR
DEVELOPMENT

Artificial intelligence technologies have profoundly transformed not only the flow of daily life in recent years, but also our economic, social, and institutional structures. This rapid development offers new opportunities across a wide range of areas, from data analytics to automation, and from public services to private sector applications, while also bringing significant legal uncertainties. Most of our traditional laws were drafted without anticipating the existence of such dynamic and autonomous decision-making systems.

At a time when rules are struggling to keep pace with technology, critical questions arise regarding the boundaries within which artificial intelligence will operate and how the liability regime will be determined. Updating existing legislation and creating new legal frameworks is becoming inevitable in order to both protect individual rights and support the development of innovative technologies.

Therefore, today, we must approach the relationship between artificial intelligence and law not merely as a process of adaptation, but as a strategic transformation that shapes our social future. A comprehensive approach involving legislators, industry representatives, and academia will lay the foundation for a robust legal infrastructure that ensures the safe development of technology while protecting citizens' rights.

LATEST NEWS

BILL CONTAINING ARTIFICIAL INTELLIGENCE REGULATIONS SUBMITTED TO THE TURKISH GRAND NATIONAL ASSEMBLY

This new bill submitted to the Grand National Assembly of Turkey, which includes artificial intelligence (AI) regulations, aims to comprehensively regulate the legal framework for AI technologies and the measures and sanctions that should be envisaged in this context for the first time, integrating them into legislation. This initiative is a critical development for the legal and business worlds, as it has the potential to fill a significant gap in technology law and will directly impact corporate compliance processes.

This step is part of efforts to align with global developments such as the European Union's pioneering AI Act regulation. Furthermore, it is an important step for the medium-term program for the 2026-2028 period, published in the Official Gazette on September 7, 2025, regarding the alignment of the KVKK with the GDPR and the preparatory work planned on artificial intelligence.

With this Proposal submitted to the Grand National Assembly of Turkey on November 7, 2025:

1. It is intended to clarify the legal framework by adding the definition of “artificial intelligence system” to Law No. 5651 on the Regulation of Publications Made on the Internet and the Fight Against Crimes Committed Through These Publications.

2. By regulating the criminal liability regime, the aim is to consider the user who directs artificial intelligence systems to commit a crime as the “perpetrator.” The proposal text stipulates that the person who gives AI commands containing criminal elements shall be directly considered the perpetrator of the act.

3. It is intended to make it mandatory to block access to and remove content generated by artificial intelligence (that violates personal rights, threatens public safety, or is of a deepfake nature) within 6 hours.

4. It is intended to make it mandatory to add the phrase “generated by artificial intelligence” to fake videos, audio, and images (deepfakes) produced by AI.

5. The use of discriminatory data sets containing prejudice based on race, gender, religion, etc., in AI training is to be prohibited as a “data security crime” and “data breach.”

6. The aim is to grant the Information and Communication Technologies Authority (BTK) the authority to intervene urgently by blocking access to AI content that threatens public order and election security, and to impose administrative fines on individuals who act in violation of these obligations.

7. It is planned to increase the penalties for developers who enable crimes to be committed through the design or training of the system by half.

8. Provisions have been made to impose obligations on artificial intelligence service providers, such as establishing content verification mechanisms to prevent the production of false and manipulative information and ensuring the transparency of training data sets.

The relevant draft text can be accessed [here](#).



LATEST NEWS

ISTANBUL GOVERNORATE'S DECISION REGARDING THE RECORDING OF UNINTERRUPTED VIDEO AND AUDIO FOR 24 HOURS

Among the decisions announced following the Food Safety Meeting in Istanbul, the requirement for all businesses to record video footage continuously for 24 hours and retain the recordings for 30 days stands out.

Although the initial announcements included the phrase “audio and video recording,” the Governorate's updated official text only mentions the requirement for video recording.

Monitoring activities on this scale are likely to raise serious issues in terms of privacy, personal data protection, legality, proportionality, and certainty.

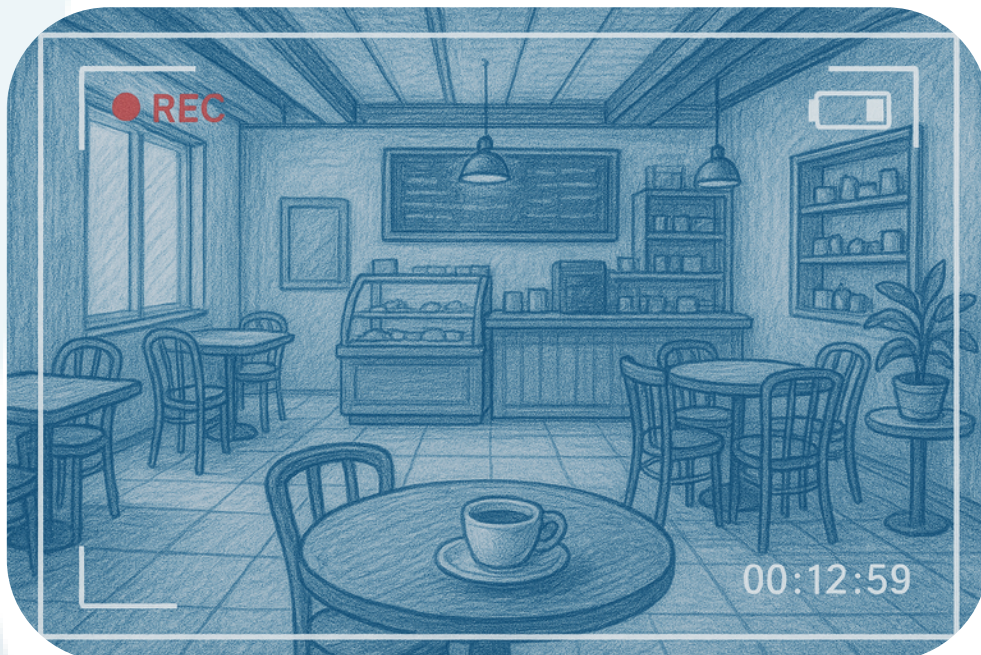
Indeed, the principle of data minimization, which requires that only the minimum amount of data necessary be processed, should be adopted by all data controllers. The guidance provided by the Board and judicial decisions also follows this approach.

Recording 24/7 in all businesses may result in excessive and unnecessary data processing and may violate the principle of data minimization.

Setting the retention period at 30 days is considered the ideal duration as it will not create unnecessary storage.

In conclusion, while the removal of the term “audio recording” is important, the requirement for video recording alone is controversial in terms of the principles of legality, proportionality, and certainty, and if the regulation is subject to judicial review, it is highly likely to be overturned.

You can access the relevant news from the Istanbul Governorate [here](#).



LATEST NEWS

A PROPOSAL FOR AMENDMENTS TO THE INTERNET LAW NO. 5651 HAS BEEN SUBMITTED TO THE TURKISH GRAND NATIONAL ASSEMBLY

A proposed amendment to Law No. 5651 on the Regulation of Publications Made on the Internet and the Fight Against Crimes Committed Through These Publications has been submitted to the Turkish Grand National Assembly.

In line with the annulment decision taken by the Constitutional Court in October 2023, the proposal mainly changes the following points:

When the “removal of content” measure is applied, the content in question can be removed from the internet in a reversible manner if necessary.

The title of the provision of the Law annulled by the Constitutional Court, “Removal of content and blocking of access,” is changed to “Violation of personal rights.” According to the revised provision, individuals who claim that their personal rights have been violated due to published content may apply to the criminal court of first instance for the removal of the content and/or blocking of access.

If requested by individuals claiming that their personal rights have been violated due to published content, the criminal court of peace may, without the need for a detailed investigation, decide within 24 hours to remove the content and/or block access in cases where the violation is apparent at first glance, and may also decide not to link the applicant's name to the internet addresses involved in the violation. The decision will include the search engines to be notified. If the violation is not apparent at first glance without the need for a detailed investigation, the request will be rejected.

The magistrate judge will only rule on the publication in which the violation occurred within the scope of this provision. A decision cannot be made to block access to the entire publication on the website. However, if it is determined that the infringement cannot be prevented by blocking access to the content by specifying the URL address, or if the decision to remove the content has not been implemented, a decision may be made to block access to the entire publication on the website, provided that the reason is clearly stated.

The decision issued by the criminal court of first instance shall be sent directly to the Access Providers Association to be notified to the access providers and related content and hosting providers. This decision shall be notified by the Association to the access providers and related content and hosting providers. Upon notification, the decision shall be implemented immediately and within 4 hours at the latest.

The judge whose decision is being appealed or the competent authority authorized to review the appeal may hear the parties if deemed necessary.

You can access the relevant draft text [here](#).



LATEST NEWS

DIGITAL ECONOMY PARTNERSHIP AGREEMENT BETWEEN THE GOVERNMENTS OF THE MEMBER STATES OF THE ORGANIZATION OF TURKISH STATES

A bill approving the Digital Economy Partnership Agreement, which includes specific provisions on personal data transfer among the Organization of Turkic States, has been submitted to the Turkish Grand National Assembly.

The Organization of Turkic States (OTS) is taking an important step towards strengthening digital trade and addressing data security on a common ground. The Digital Economy Partnership Agreement between the Governments of the Member States of the Organization of Turkic States was signed in Bishkek on November 6, 2024, and is now in the process of ratification in our country.

Article 19 of the agreement gives special attention to the protection of personal data. Accordingly, the signatory countries are expected to:

- Have a national legal framework for personal data protection,
- Establish clear rules for cross-border data transfer,
- Make information about individuals' rights and businesses' obligations publicly available,
- Increase transparency in data protection practices.

In this context, Article 19 of the Agreement reads as follows:

"(1) The Parties recognize the economic and social benefits of protecting personal data and its contribution to increasing consumer confidence in electronic commerce.

(2) Each Party shall establish or maintain a national legal framework for the protection of personal data, including personal data transferred across borders.

(3) Each Party shall make data protection laws and regulations publicly available and easily accessible and shall designate a competent data protection authority:

(a) how individuals can seek redress in the event of a violation of their data protection rights; and

(b) the legal obligations to which the business is subject regarding the protection of personal data and information about the personal data protections provided by the state, including any guidelines for their implementation.

(4) Each Party shall encourage businesses in its country to publish their policies and procedures regarding the protection of personal data, including on the internet.

(5) Recognizing that the Parties may adopt different legal approaches to the protection of personal data, the Parties shall endeavor to exchange information and share experiences regarding such mechanisms applied under their jurisdictions."

Full members of the TDT are: Turkey, Azerbaijan, Kazakhstan, Kyrgyzstan, and Uzbekistan.

Observer members are Hungary, Turkmenistan, and the Turkish Republic of Northern Cyprus.

You can access the bill dated 11/27/2025 regarding the approval of the agreement [here](#).



LATEST NEWS

RECOMMENDATIONS FROM THE KVKK FOR NOVEMBER 30TH, COMPUTER SECURITY DAY

The KVKK has issued a series of recommendations and reminders specifically for November 30 Computer Security Day.

The KVKK has outlined the basic steps you can take to ensure the security of your computers and, consequently, your personal data, as follows:

- **SETTINGS**

Configure the settings of the programs you use on your computer with security in mind.

- **FIREWALL**

A firewall is one of the basic measures that can be used to protect your computer against unauthorized access attempts over the internet.

- **PERIODIC CHECKS**

Regularly scan the files on your computer and make sure to use up-to-date software.

- **SAFE WEB**

Use security tools designed to block malicious websites. Also, stay away from websites that offer illegal or risky content.

- **EXTERNAL DEVICES**

To prevent the spread of malicious software, ensure that external devices such as USB drives come from a reliable source before using them.

- **EMAIL**

Do not open emails or attachments from unknown sources or whose security you cannot verify.

- **PHISHING ATTACKS**

Be cautious of phishing attacks that attempt to deceive you with fake announcements and links.

- **SCREEN LOCK**

Even if you step away from your computer for a short time, do not forget to lock it.

You can access the relevant article [here](#).



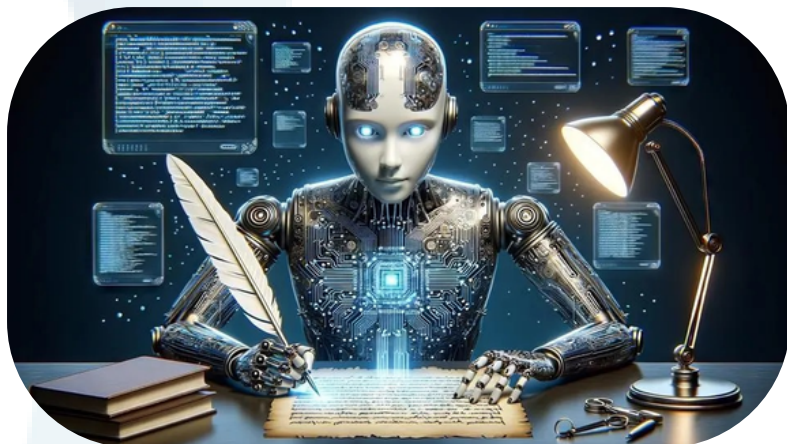
LATEST NEWS

THE PERSONAL DATA PROTECTION AUTHORITY HAS PUBLISHED THE “GUIDE ON GENERATIVE ARTIFICIAL INTELLIGENCE AND THE PROTECTION OF PERSONAL DATA (15 QUESTIONS)”

The Personal Data Protection Authority (“Authority”) published the “Guide on Generative Artificial Intelligence and the Protection of Personal Data (15 Questions)” (“Guide”) on November 24, 2025. The relevant Guide provides descriptive and explanatory information about Generative Artificial Intelligence (“AIA”) and encourages a privacy-friendly approach in the development and use of these systems. It also provides guidance to actors who are data controllers in terms of personal data processing activities carried out throughout the life cycle.

The topics and questions covered in the relevant Guide are as follows:

- Some Concepts and Definitions Related to Artificial Intelligence
- Purpose and Scope
- What is Generative Artificial Intelligence?
- How is Content Production Achieved in Generative Artificial Intelligence Systems?
- What Stages Does the Life Cycle of a Generative Artificial Intelligence Model Consist of?
- In Which Areas Is Generative Artificial Intelligence Used?
- What Risks Does the Use of Generative Artificial Intelligence Pose?
- Is Personal Data Processed in Generative Artificial Intelligence Systems?
- How Should the Data Controller and Data Processor Be Determined Within the Scope of the Life Cycle of Generative Artificial Intelligence Systems?
- How Should the General Principles of Personal Data Processing Be Applied in Generative Artificial Intelligence Systems?
- How Should the Conditions for Processing Personal Data (Legal Basis) in Generative Artificial Intelligence Systems Be Determined?
- How Should the Transfer of Personal Data Abroad in Generative Artificial Intelligence Systems Be Assessed?
- How Can Transparency Be Ensured in the Context of Generative Artificial Intelligence Systems?
- How Can the Rights of Data Subjects Be Exercised in the Context of Generative Artificial Intelligence Systems?
- What Should Be Considered Regarding the Security of Personal Data in Generative Artificial Intelligence Systems?
- What Should Individuals Pay Attention to Regarding the Protection of Personal Data When Using Generative Artificial Intelligence Applications in Everyday Life?
- What Precautions Can Parents Take for Children Using Generative Artificial Intelligence Tools?



You can access the relevant guide [here](#).

GLOBAL NEWS

UNICEF HAS PUBLISHED A NEW REPORT ON THE PROTECTION OF CHILDREN IN ONLINE GAMES

UNICEF has released a new report on protecting children in online games. The report emphasizes that children's rights to both play and be protected from violence in online gaming environments must be safeguarded; to achieve this goal, the development of effective prevention, detection, and intervention mechanisms is essential.

The report analyzes how violent organizations instrumentalize online gaming ecosystems to involve children in propaganda and violent actions.

It highlights how the social and technical features of games can be used by these organizations to reach, influence, and organize children.



The report, which highlights the need for a comprehensive approach to addressing these risks, presents recommendations for four key stakeholder groups: international organizations, governments and regulatory bodies, gaming companies and platforms, and civil society, educators, and parents. In this regard, all actors are called upon to act with a shared sense of responsibility to ensure that online gaming environments remain inclusive, creative, and safe for children.

You can access the relevant report [here](#).

GLOBAL NEWS

THE EUROPEAN COMMISSION PUBLISHED A DOCUMENT TITLED “DATA UNION STRATEGY – UNLOCKING DATA FOR ARTIFICIAL INTELLIGENCE.”

The European Commission has published a document titled “Data Union Strategy – Unlocking Data for Artificial Intelligence.” The Data Union Strategy focuses on three priority areas: increasing access to data for artificial intelligence, simplifying data rules, and strengthening the European Union's global position on international data flows. It is stated that the Data Union Strategy, to the extent appropriate, can provide policymakers and industry, particularly SMEs, with a framework to guide them in removing barriers and completing the single market for data.

The relevant guide includes the following statements regarding the current importance of artificial intelligence:

Artificial intelligence is transforming the global economy, and the EU needs large amounts of high-quality data to remain competitive and foster innovation. Without this data, the EU cannot develop powerful AI models, optimize healthcare or energy systems, or maintain its industrial leadership.

For small and medium-sized enterprises in particular, better data access will be crucial for scaling up and maintaining competitiveness. By investing in important legislation such as the Data Act and common European data spaces, the European Union has laid solid foundations for creating a secure and interoperable single market for data.

You can access the relevant document [here](#).

