NUMBER: 58

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

DATA & TECHNOLOGY LAW BULLETIN

DECEMBER 2025

LATEST NEWS

- Presidential Decrees on Corporate Distribution Related to Cybersecurity and Artificial Intelligence Published.
- Decision from the Istanbul 9th Civil Commercial Court Regarding the Principle of Data Minimization.
- New Issue of the Personal Data Protection Journal Published.
- For the first time in Turkey, an arrest warrant was issued in accordance with the Cyber Security Law as a result of a cyber operation involving the Cyber Security Presidency.
- Personal Data Breaches Reported in December

GLOBAL NEWS

- UNICEF Releases Updated Version of Guide on Artificial Intelligence and Children.
- World Bank Group Releases Study "Digital Progress and Trends Report 2025: Strengthening the Foundations of Artificial Intelligence."

THE INCREASING ROLE OF LEGISLATION IN CYBERSECURITY

With the acceleration of digitalization, many sectors—from public services to financial systems, healthcare infrastructure to critical industries—are operating in cyberspace, making cybersecurity a strategic priority. The increasing volume of data, remote working models, and the proliferation of cloud-based systems are increasing both the number and complexity of cyber threats, prompting governments and regulatory authorities to create stronger and more comprehensive legal frameworks.

On a global scale, many countries, particularly the European Union, are updating their cybersecurity legislation and expanding binding obligations. The protection of critical infrastructure, supply chain security, incident reporting obligations, and administrative sanctions are at the heart of these regulations. Similarly, in Turkey, legislative efforts to strengthen cybersecurity have gained momentum, with the protection of personal data and the security of critical infrastructure becoming focal points.

In light of these developments, cybersecurity is no longer just a technical field under the responsibility of IT departments; it has become a critical issue that concerns the entire organization, from top management to legal and compliance departments. Closely following current legislation and aligning corporate processes with these regulations is of great importance in terms of both reducing legal risks and ensuring the sustainable protection of digital assets.

LATEST NEWS

PRESIDENTIAL DECREES ON CORPORATE DISTRIBUTION RELATED TO CYBERSECURITY AND ARTIFICIAL INTELLIGENCE PUBLISHED

On December 25, 2025, Presidential Decrees No. 191 and 192 were published in the Official Gazette, introducing new regulations and developments in the fields of artificial intelligence and cybersecurity. With these updates, the distribution of institutional responsibilities and authorities related to artificial intelligence has become more clearly defined.

- With the regulations introduced by Presidential Decree No. 191, the name of the National Technology Directorate operating within the Ministry of Industry and Technology was changed to the National Technology and Artificial Intelligence Directorate. The duties of the Directorate General were defined as follows:

-Preparing policies and strategies for the reliable, ethical, and responsible development and use of artificial intelligence technologies and coordinating their implementation.

-Conducting studies to increase data, infrastructure, and human resource capacity in the field of artificial intelligence, contributing to programs and mechanisms that support initiatives and R&D activities.

- To carry out work on the preparation and development of necessary legislation in the field of artificial intelligence, to develop international cooperation, and to ensure the coordination of the artificial intelligence ecosystem at the national level,

- To establish policies and strategies for the development of data center and cloud computing infrastructure in Turkey, to determine criteria and standards for data centers, and to prepare and implement regulations for certification and authorization.

CUMHURBAŞKANLIĞI KARARNAMESİ

- With the regulations introduced by Presidential Decree No. 2192, the Public Artificial Intelligence Directorate General was established within the Presidency of Cyber Security, clearly defining a comprehensive and centralized area of authority for artificial intelligence applications in the public sector. Accordingly, the duties of the Directorate are as follows:

-To carry out legislative work on artificial intelligence applications in the public sector,

-To contribute to the preparation of national policies, strategies, and action plans in the field of artificial intelligence, as well as to the harmonization of national legislation with international regulations, and to participate in ecosystem development activities,

-Establishing principles, procedures, and standards for data governance, covering the management of processes from data creation to destruction within the scope of digital government and the use of artificial intelligence technologies in the public sector,

-Leading the way in artificial intelligence applications in the public sector, identifying the relevant requirements together with the relevant institutions, implementing a common data area infrastructure, determining the quality criteria and standards for data to be used in applications, and granting compliance.

When Presidential Decrees No. 191 and 192 are considered together:

It is seen that the authorities and responsibilities related to artificial intelligence are structured through two separate administrative actors, in a dual structure. However, at the current stage, it is seen that no preference has been made towards establishing an independent administrative authority in the field of artificial intelligence. Instead, an approach has been adopted whereby the existing administrative structures are strengthened, and governance functions related to artificial intelligence are structured through a distributed and dual administrative model.

LATEST NEWS

DECISION OF THE ISTANBUL 9TH COMMERCIAL COURT OF FIRST INSTANCE REGARDING THE PRINCIPLE OF DATA MINIMIZATION

İThe trial process regarding the Istanbul 9th Civil Commercial Court Case No. 2025/458, Decision No. 2025/536 is as follows:

In a previous inheritance case between the parties, the court requested the bank account transactions of the deceased and related persons for the previous 10 years.

Later, in another case joined with this case, a letter was sent to the bank requesting that the previous response to the inquiry be resubmitted. Upon this request, the bank sent its response to the inquiry and submitted the current and unsolicited account movements of the persons concerned to the file. These documents were leaked from the case file and published on a website. Upon realizing the situation, the bank requested that the data be deleted from the file and UYAP and blocked access to the website. In response, the plaintiffs in this case claimed that the bank had disclosed personal data constituting customer confidentiality and sought moral damages.

The court of first instance rejected the claim for moral damages, stating that the bank had inadvertently submitted the documents to the file and had subsequently taken corrective measures. At the appeal stage, the Regional Court of Appeals rejected the appeal, finding that the bank had no intent to violate data protection.

Following a detailed review by the Court of Cassation during the appeal stage, it was determined that the bank was both a trust institution and a data controller under the Personal Data Protection Law No. 6698 (“KVKK”); and that it is obliged to comply with the principles of confidentiality, proportionality, and purpose limitation under both Article 73 of the Banking Law No. 5411 and the KVKK.

The court ruled that the bank's submission of extensive account statements belonging to the plaintiffs to the case file, exceeding the scope of the subpoena and the requested date range, was unlawful. It stated that the reasoning accepted in the first instance and appellate court decisions that “the letter was not clear” was unfounded, and the first instance and appellate court decisions were overturned and annulled.

Following the Supreme Court's decision to overturn the ruling, the relevant court of first instance, the Istanbul Commercial Court of First Instance, complied with the overturning decision and found that the submission of personal data requested by the bank to the case file was unlawful in terms of personal rights. In accordance with the general provisions of the KVKK and the provisions of the Turkish Civil Code regarding the protection of personality, it awarded moral damages totaling TL 100,000, consisting of TL 50,000 for each real person plaintiff. However, the claims for moral damages by the corporate plaintiffs were rejected on the grounds that the KVKK protects information relating to natural persons in the legal sphere but does not protect information relating to legal persons, and also on the grounds that these companies were not customers of the bank under the Banking Law.

LATEST NEWS

THE NEW ISSUE OF THE PERSONAL DATA PROTECTION JOURNAL HAS BEEN PUBLISHED

The Journal of Personal Data Protection, a peer-reviewed scientific and academic journal published twice a year by the Personal Data Protection Authority, provides an interdisciplinary, scientific publishing platform for academics, professionals, and other stakeholders engaged in research on personal data protection to present their work.

The fourteenth issue of the journal, which features research and review articles on personal data protection, privacy, data protection law, and personal data security, includes:

- The Country-Outside Effect Principle: An Examination Through the GDPR
- The Transformation of Digital Privacy: A Child Rights Perspective on EU and Türkiye's Regulatory Frameworks and Recent Developments
- Data Security in the Light of Twin Transformation: Increasing Data Load and Privacy Risks in Green and Digital Transformation
- How Can Privacy-Enhancing Technologies Promote the Development and Use of Artificial Intelligence Technology Without Compromising Privacy? A Policy Proposal for Turkey

These articles are made available to interested parties to contribute to the field of personal data protection.

This Personal Data Protection Journal, published by the Personal Data Protection Board, is accessible to everyone in electronic format and can be accessed via the "Publications" section on the official website of the Personal Data Protection Board or via the link dergipark.org.tr/kvkd.

LATEST NEWS

FOR THE FIRST TIME IN TURKEY, AN ARREST WARRANT WAS ISSUED AS A RESULT OF A CYBER OPERATION INVOLVING THE CYBER SECURITY DIRECTORATE

For the first time in Turkey, an arrest warrant was issued under the Cyber Security Law as a result of a cyber operation involving the Cyber Security Directorate.

According to a news report broadcast yesterday on TRT, in summary:

As part of the first cyber operation involving the Cyber Security Directorate, an arrest warrant was issued under the Cyber Security Law No. 7545 against suspects who attempted to gain unauthorized access to public institution systems by targeting personal data, in coordination with the National Intelligence Organization (MİT).

Under the coordination of the National Intelligence Organization, the Cyber Security Directorate, the Financial Crimes Investigation Board (MASAK), and the Gendarmerie General Command carried out a comprehensive cyber espionage operation.

MİT's investigations revealed that unauthorized access to citizens' personal data had been used to systematically transfer data illegally as part of espionage activities. It was reported that the Cyber Security Directorate provided MİT with the necessary technical support during the operations.

In investigations conducted by MASAK, it was determined that illegal income flows were fragmented through cryptocurrency transfers, payments were directed to foreign-based platforms, and money movements were concealed using multi-stage transfer methods. It was stated that the financial flows in question were recorded as part of the investigation.

As part of the investigation conducted by the Ankara Chief Public Prosecutor's Office, eight websites found to be hosting illegally obtained data were seized and shut down, and technical devices such as data storage devices were confiscated.

LATEST NEWS

PERSONAL DATA BREACHES REPORTED DURING DECEMBER

BEYÇELİK HOLDİNG A.Ş. VE GRUP ŞİRKETLERİ

Data controller: Beyçelik Holding Inc., Bak Energy Production Inc., Ber Energy Production Inc., BEWEN Energy Inc., Beyçelik Elawan Renewable Energy Production Inc. Beyçelik Gestamp Automotive Industry Inc., Beyçelik Gestamp Chassis Automotive Industry Inc., Beyçelik Gestamp Technology and Mold Industry Inc., Beyçelik Insurance Brokerage Services Inc., Çelikform Gestamp Automotive Inc., Gesbey Energy Turbine Tower Production Industry and Trade Inc., Gescrap Turkey Metal Industry and Trade Inc. Inc., Sabaş Electricity Production Inc., Warmhaus Heating and Cooling Systems Industry and Trade Inc., YGT Electricity Production Inc. reported data breaches to the Authority, summarizing as follows:

- The breach occurred as a result of ransomware being installed on Beyçelik Gestamp Otomotiv Sanayi AŞ's servers on 04.12.2025, encrypting their systems.
- The groups of individuals affected by the breach are not yet known.
- It is not technically possible at this stage to separate the categories of personal data stored on the servers that were attacked; investigations are ongoing.
- The number of individuals affected by the breach has not yet been determined; investigations are ongoing.

information is provided.

While the investigation into the matter is ongoing, the Personal Data Protection Board's Decision No. 2025/2385 dated 12/11/2025 has decided that the relevant data breach notifications shall be published on the Authority's website.
You can access the relevant breach notification here .

DEM İLAÇ SANAYİ VE TİCARET A.Ş.

In summary, the data breach notification submitted to the Board by Dem İlaç Sanayi ve Ticaret A.Ş., acting as the data controller, states that:

- The data controller was subjected to a ransomware attack on December 7, 2025,
- The cyber threat actor allegedly obtained approximately 1 TB of sensitive data,
- Investigations into the breach are ongoing within the data controller,
- The groups of individuals affected by the breach are employees, users, customers/potential customers,
- It is stated that the threat actor gained access to all systems, and therefore the personal data that may have been affected is broadly specified; in this context, the affected data may include identity, communication, location, personal details, legal proceedings, customer transactions, physical location security, transaction security, risk management, finance, professional experience, marketing, visual and audio recordings, health information, criminal convictions, and security measures.
- The number of individuals affected by the breach has not yet been determined; the investigation is ongoing;
- Relevant individuals can obtain information via www.demilac.com.tr or the call center,

information is provided.

While the investigation into the matter is ongoing, the Personal Data Protection Board's Decision No. 2025/2387 dated 11.12.2025 has decided that the data breach notification in question should be published on the Institution's website.
You can access the relevant breach notification here .

LATEST NEWS

PERSONAL DATA BREACHES REPORTED DURING DECEMBER

DMR OTOMOTİV KİRALAMA SANAYİ VE TİCARET LTD. ŞTİ.

In summary, the data breach notification submitted to the Board by DMR Otomotiv Kiralama Sanayi Ve Ticaret Limited Şirketi, acting as the data controller, states that:

- The data controller was subjected to a ransomware attack on December 7, 2025.
- The breach occurred at Dem İlaç Sanayi ve Ticaret A.Ş., a group company of the data controller.
- The cyber threat actor allegedly obtained approximately 1 TB of sensitive data,
- Investigations into the breach are ongoing within the data controller,
- The groups of individuals affected by the breach are employees, users, customers/potential customers,
- Personal data that may have been affected is broadly specified, as it is stated that the threat actor gained access to all systems; in this context, the affected data may include identity, communication, location, personal details, legal proceedings, customer transactions, physical location security, transaction security, risk management, finance, professional experience, marketing, visual and audio recordings, health information, criminal convictions, and security measures.
- The number of individuals affected by the breach has not yet been determined; the investigation is ongoing;
- Relevant individuals can obtain information via www.demilac.com.tr or the call center,

information is provided.

While the investigation into the matter is ongoing, the Personal Data Protection Board's Decision No. 2025/2388 dated 11.12.2025 has decided that the data breach notification in question should be published on the Institution's website.

You can access the relevant breach notification here .

PHARMADA İLAÇ SANAYI VE TICARET A.Ş.

In summary, the data breach notification submitted to the Board by Pharmada İlaç Sanayi ve Ticaret A.Ş., acting as the data controller, states that:

- The data controller was subjected to a ransomware attack on December 7, 2025.
- The breach occurred at Dem İlaç Sanayi ve Ticaret A.Ş., a group company of the data controller.
- The cyber threat actor allegedly obtained approximately 1 TB of sensitive data,
- Investigations into the breach are ongoing within the data controller,
- The groups of individuals affected by the breach are employees, users, customers/potential customers,
- Personal data that may have been affected is broadly specified, as it is stated that the threat actor gained access to all systems; in this context, the affected data may include identity, communication, location, personal details, legal proceedings, customer transactions, physical location security, transaction security, risk management, finance, professional experience, marketing, visual and audio recordings, health information, criminal convictions, and security measures.
- The number of individuals affected by the breach has not yet been determined; the investigation is ongoing;
- Relevant individuals can obtain information via www.demilac.com.tr or the call center,

information is provided.

While the investigation into the matter is ongoing, the Personal Data Protection Board's Decision No. 2025/2389 dated 11.12.2025 has decided that the data breach notification in question should be published on the Institution's website.

You can access the relevant breach notification here .

LATEST NEWS

PERSONAL DATA BREACHES REPORTED DURING DECEMBER

BALIKESİR ULUDAĞ TURİZM TAŞ. İNŞ. TİC. LTD. ŞTİ.

The data breach notification submitted to the Board by Balıkesir Uludağ Turizm Taş. İnş. Tic. Ltd. Şti., acting as the data controller, summarizes as follows:

- The breach occurred between December 1, 2025, and December 5, 2025, and was detected on December 6, 2025, at 3:52 p.m.
- The breach occurred as a result of a brute-force attack on the data controller's authorized user account on the portal management login page, which resulted in unauthorized access to the system.
- The individuals who gained unauthorized access claimed that they had obtained company information and notified company managers via SMS.
- The exact number of individuals affected by the breach is unknown, but the attacker claims to have obtained more than 10 million pieces of data,
- The group of individuals affected by the breach includes employees, subscribers/members, and customers,
- The data controller has stated that the categories of personal data affected by the breach are identity and contact information, However, it is alleged that the attacker obtained bus trip data (departure/arrival bus station, date, time) belonging to the data controller, personal data of passengers on bus trips, SMS data logs, Turkish ID numbers, phone numbers, first names, last names, passwords, and member numbers of all members, job application logs, employee information, and lost property data.

While the investigation into the matter is ongoing, the Personal Data Protection Board's Decision No. 2025/2391 dated 11.12.2025 has decided that the notification of the data breach in question should be published on the Authority's website.

You can access the relevant breach notification here .

ULUDAĞ ELEKTRIK DAĞITIM AŞ

In the data breach notification submitted to the Board by Uludağ Elektrik Dağıtım AŞ, acting as the data controller, it is summarized that:

- The breach occurred on August 5, 2025, and was detected on August 18, 2025.
- A data set containing the information of the data controller's subscribers was detected on a platform used by threat actors on the dark web for file sharing.
- The data set in question contained 57 data categories, including subscriber number, name and surname, partial address, consumption information, meter information, and other mostly technical data, as well as personal data, and the data matched the records stored in the system.
- The root cause of the breach was that malicious threat actors gained access to the system, which could only be accessed by logging in with a password and an SMS verification code that had to be obtained each time, through illegal means.
- The exact number of individuals affected by the breach could not be determined, but the number of queries performed was 899,890.
- The group of individuals affected by the breach consists of subscribers/members,
- Affected individuals can contact dpo@uedas.com.tr to obtain information about the data breach.

This information has been provided.

While the investigation into the matter is ongoing, the Personal Data Protection Board's Decision No. 2025/2443 dated December 25, 2025, has decided that the notification of the data breach in question shall be published on the Authority's website.

You can access the relevant breach notification here .

GLOBAL NEWS

UNICEF RELEASES UPDATED VERSION OF ITS GUIDE ON ARTIFICIAL INTELLIGENCE AND CHILDREN

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 .

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GLOBAL NEWS

WORLD BANK GROUP RELEASES STUDY "DIGITAL PROGRESS AND TRENDS REPORT 2025: STRENGTHENING THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE."

The World Bank Group's "Digital Progress and Trends Report 2025: Strengthening the Foundations of Artificial Intelligence" examines how low- and middle-income countries can leverage artificial intelligence to achieve inclusive and sustainable development.

In this context, the report addresses the fundamental elements of AI adoption, adaptation, and innovation processes:

- Connectivity (infrastructure)
- Computing (processing power)
- Context (training data, algorithms, and applications)
- Competence (digital skills)

.

This published report consists of the following sections and also includes various work summaries and case studies:

- Overview
- Section 1: Using Artificial Intelligence for Development: Does it Work?
- Section 2: Connectivity
- Section 3: Computing
- Section 4: Context: Education Data and Adapting the Artificial Intelligence Model
- Section 5: Competency: Digital Skills
- Section 6: Conclusion
- Appendix: Thematic Case Study Summaries
- Case Study 1: Exploring the Revolutionary Potential of AI for Education Systems in Low- and Middle-Income Countries
- Case Study 2: Using Artificial Intelligence for Efficiency: Transforming the Agriculture and Energy Sectors
- Case Study 3: Colleague, Coach, or Competitor? How Artificial Intelligence is Transforming the Future of Digitally Delivered Services?

You can access the related study here.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership