

EGE ÇAKIRCA

Attorneys at Law

JUNE'26

DATA PROTECTION BULLETIN



**AUTHORITY
DECISIONS AND
ANNOUNCEMENTS**



**GLOBAL
DEVELOPMENTS**



**JUDICIAL
DECISIONS**

This bulletin, prepared by Ege Çakırca Attorneys at Law in relation to legal developments occurring in the field of personal data protection law during June and July 2026, is intended solely for general informational purposes and does not constitute legal advice, a legal opinion, an assessment, or consultancy services of any kind. As the contents herein have not been prepared for application to any specific matter, they do not give rise to an attorney-client relationship.

No express or implied representation, undertaking, or warranty is given as to the accuracy, currency, completeness, or fitness for any particular purpose of the information and assessments contained herein.

Before taking any action in reliance on these contents, professional advice should be sought from a qualified legal practitioner, taking into account the specific circumstances of the relevant matter. Any risk or liability arising from actions taken otherwise shall rest exclusively with the relevant person.

Our firm, its partners, employees, and lawyers accept no liability whatsoever for any direct or indirect loss or damage arising from the use or interpretation of these contents or from any decisions made in reliance thereon.

— Authority Decisions and Announcements

1 Announcement on the Use of Security Cameras in Workplaces

DECISION DATE: 29.04.2026

PUBLICATION DATE: 02.06.2026



In its announcement, the Personal Data Protection Authority (the “**Authority**”) stated that security cameras may be used in workplaces for purposes such as ensuring occupational health and safety, maintaining workplace security, and preventing criminal activity. However, the Authority emphasised that the recording of employees and other individuals present in the workplace constitutes the processing of personal data.

Accordingly, employers using video surveillance systems must comply with the personal data processing conditions and general principles laid down in Law No. 6698 on the Protection of Personal Data. In particular, camera footage must be processed for specified, explicit, and legitimate purposes; be relevant, limited, and proportionate to those purposes; and be retained only for the period necessary to fulfil the purposes for which it is processed.

The announcement further emphasises that camera systems should not be used for purposes other than those for which they were installed, such as monitoring employees’ attendance or performance. The use of such systems must therefore be assessed in accordance with the principles of suitability, necessity, and proportionality.

The Authority also states that, depending on the particular circumstances of each case, the use of cameras may be permissible in areas presenting security risks, such as entrances and exits, warehouses, and cash-handling areas. However, cameras should not be installed in areas where individuals have a heightened expectation of privacy, including toilets, changing rooms, prayer rooms, and rest areas. The recording of audio constitutes a more intrusive interference with the right to privacy and must therefore be assessed with particular caution.

In conclusion, the use of security cameras in workplaces is not prohibited per se. Nevertheless, such use must pursue a legitimate purpose, be proportionate to that purpose and not infringe upon the reasonable expectation of privacy of data subjects. The Authority has stated that, where the applicable obligations are not complied with, enforcement

measures may be taken against data controllers, including the imposition of administrative fines.

The full text of the announcement is available [here](#).

2 Announcement on the Use of Security Cameras in Apartment Buildings and Residential Complexes

PUBLICATION DATE: 08.06.2026

In its announcement, the Personal Data Protection Authority stated that security cameras may be used in apartment buildings and residential complexes for the purposes of ensuring general security, protecting common areas, and preventing acts such as theft or damage to property. The Authority further emphasised that the recording of individuals’ images through video surveillance systems constitutes the processing of personal data within the scope of Law No. 6698 on the Protection of Personal Data.

The use of cameras in the common areas of apartment buildings and residential complexes may, depending on the circumstances of the specific case, be based on legal grounds such as the necessity of processing for the establishment, exercise, or protection of a right or for the legitimate interests pursued by the data controller, provided that the fundamental rights and freedoms of the data subject are not prejudiced. In all cases, however, such processing must comply with the general principles set out in the Law.

The announcement places particular emphasis on the principles of proportionality and data minimisation. It states that cameras must be positioned in a manner that does not infringe upon residents’ reasonable expectation of privacy and must not be installed in locations from which the interiors of individual units may be viewed, in stairwells, or at points that would result in the unnecessary recording of excessively broad areas.

The Authority further stated that video surveillance systems should be used solely for security purposes and that features such as facial recognition, audio recording, or other functionalities that may constitute a more serious interference with the right to privacy should be avoided. Although elevators constitute common areas, the announcement emphasises that, given their confined and enclosed nature, the justification for installing cameras in such areas must be clearly established.

In conclusion, the use of security cameras in apartment buildings and residential complexes is not prohibited; however, such use must be relevant to, limited to, and proportionate to the stated purpose, and must be lawful. The Authority noted that, in cases of non-compliance with these obligations, enforcement measures may be taken, including the imposition of administrative fines.

The full text of the announcement is available [here](#).

3 Public Announcement on Live Broadcasts by Municipalities for Tourism Promotion Purposes

PUBLICATION DATE: 23.06.2026

 In its announcement, the Personal Data Protection Authority stated that it had received numerous reports and complaints concerning the live broadcasting, through municipal websites, of video footage captured by cameras installed by certain municipalities in streets, public squares, parks, coastal areas, and similar locations for tourism promotion purposes.

The Authority's investigations revealed that identifiable individuals' faces were visible and vehicle registration plates were legible in the relevant live broadcasts. In this context, the Authority emphasised that, even where the footage is not recorded, broadcasting it online in a manner accessible to the general public constitutes the processing of personal data as it makes such data publicly accessible.

The announcement states that, although municipalities are authorised to carry out tourism and promotion activities, such authority does not, in itself, provide a lawful basis for the live broadcasting of video footage where individuals may be identified. It further notes that the broadcasts in question cannot be regarded as public-space video surveillance activities conducted for security purposes by competent public authorities. The Authority also drew attention to the fact that the live broadcasting of areas in which individuals socialise, such as public squares, promenades, seating areas, and beaches, may interfere with the right to respect for private life. The fact that such footage is made accessible online to an unlimited number of persons also gives rise to risks of misuse and harm that may be difficult to remedy.

In conclusion, the Authority stated that municipalities must immediately cease live broadcasting activities conducted for tourism promotion purposes where such activities enable the identification of individuals and are not based on an applicable legal ground. It further emphasised that the same objective should be pursued through less intrusive alternatives, such as imaging methods that do not allow individuals to be identified or visual materials that do not contain personal data.

The full text of the announcement is available [here](#).

4 Principle Decision on the Processing of Accident Victims' Personal Data

DECISION DATE: 20.05.2026

PUBLICATION DATE: 01.07.2026

In the proceedings giving rise to the decision, the Personal Data Protection Board received numerous reports and complaints alleging that accident victims had been contacted without their consent, informed that their compensation claims could be pursued if they granted a power of attorney, and, in certain cases, that actions had been taken on their behalf without their authorisation. The decision states that, under the Attorneyship Law, the Insurance Law, and the applicable professional rules, persons and entities operating under designations such as claims consultancy companies may incur administrative and criminal liability where they unlawfully pursue compensation claims on behalf of accident victims.

From the perspective of personal data protection law, the Board principally emphasised that accident victims' personal data may be processed only lawfully and for specified, explicit, and legitimate purposes. Although such data may be processed for purposes including the conduct of judicial and administrative proceedings following an accident, the provision of medical treatment, damage assessment, vehicle repair, and insurance-related transactions, the use of such data for purposes incompatible with those for which it was collected, its disclosure to unauthorised persons, or its unlawful acquisition may constitute a breach of Law No. 6698 on the Protection of Personal Data.

The decision also separately addresses the personal data processing activities of insurance loss adjusters. It states that loss adjusters may process personal data only to the extent necessary for damage assessment, reporting, and compensation procedures. However, the disclosure of data obtained in the course of their duties to unauthorised third parties may

give rise to a breach of Law No. 6698 on the Protection of Personal Data.

In conclusion, the Board underscored the need to comply with the principles of data minimisation and purpose limitation, as well as with obligations relating to access controls, authorisation management, and data security, when processing accident victims' personal data in connection with insurance, claims management, loss adjustment, healthcare services, and legal practice. Data controllers that fail to comply with these obligations may be subject to administrative sanctions under Law No. 6698 on the Protection of Personal Data. Depending on the circumstances of the specific case, a criminal complaint may also be filed with the competent public prosecutor's office.

The full text of the decision is available [here](#).

5 Principal Decisions on Attendance Tracking Using Biometric Data

PUBLICATION DATE: 01.07.2026



The Board stated that biometric data, including fingerprints, facial recognition data, and iris and retinal scans, constitute special categories of personal data. It further noted that there is no statutory provision expressly permitting the processing of biometric data for the purpose of monitoring employee attendance.

The decision emphasises that the validity of explicit consent may be called into question due to the imbalance of power inherent in the employment relationship. It also notes that less intrusive alternatives are available, including access cards, PIN codes, RFID/NFC identification cards, and attendance sheets.

Accordingly, the Board stated that the processing of biometric data for employee attendance tracking may be incompatible with the principle of proportionality. It therefore indicated that employers should reassess their existing practices in light of the applicable legal grounds and the principles of data minimisation and data security, particularly where the same purpose may be achieved through less intrusive means.

The full text of the decision is available [here](#).

6 Investigation and Interim Measure Decision by the Turkish Competition Authority Concerning Meta

The Turkish Competition Board considered Meta's prevention of third-party generative artificial intelligence chatbots and assistants from providing services through WhatsApp to constitute a serious indication of an abuse of dominant position. To prevent irreparable harm pending its final decision, the Board imposed an interim measure on Meta.

Accordingly, Meta is required to establish conditions that do not make it practically or economically more difficult for third-party artificial intelligence service providers to offer their services through WhatsApp.

The decision demonstrates that competition authorities are subjecting digital platforms to increasingly close scrutiny, particularly as to whether the integration of their own artificial intelligence services into their platforms restricts competing service providers' access to the market.

The full text of the decision is available [here](#).

— JUDICIAL DECISIONS

1 Constitutional Court Judgment Finding a Violation in Relation to an Administrative Fine for the Processing of Publicly Disclosed Personal Data

DECISION DATE: 27.01.2026

PUBLICATION DATE: 16.06.2026

DECISION NUMBER: 2020/32193



In the case giving rise to the application, the applicant company, which operates in the insurance sector, argued that it had obtained the data subject's name, surname, and telephone number from a publicly accessible website and that the data had been made public by the data subject. The Personal Data Protection Board, however, found that the data had been used for commercial appointment scheduling and quotation purposes beyond the purpose for which they had been made public. It therefore imposed an administrative fine on the applicant company under Articles 12 and 18 of Law No. 6698 on the Protection of Personal Data. The Constitutional Court noted that Article 5(2)(d) of the Law permits the processing, without explicit consent, of personal data made public by the data subject. However, the Court observed that the Law does not expressly establish any criteria for imposing sanctions based on concepts such as the "purpose for which the data were made public", "use limited to that purpose", or "use for purposes incompatible with that purpose". The Court held that imposing, through administrative interpretation, an obligation not expressly prescribed by law and relying on that obligation as the basis for a sanction was incompatible with the principles of foreseeability and legal certainty.

Against this background, the Constitutional Court held that the administrative fine imposed on the applicant company violated the principle of legality of offences and penalties, as guaranteed under Article 38 of the Constitution.

Although the judgment does not mean that publicly disclosed personal data may, in all circumstances, be used without limitation for commercial purposes, it makes clear that, for an administrative sanction to be imposed under Law No. 6698 on the Protection of Personal Data, the obligation forming the basis of

the sanction must be prescribed by law in a clear, precise, and foreseeable manner.

The full text of the judgment is available [here](#).

2 Constitutional Court Judgment on the Principle of Legality in Administrative Fines Imposed under Law No. 6698

DECISION DATE: 27.01.2026

PUBLICATION DATE: 16.06.2026

DECISION NUMBER: 2020/3219



In the case giving rise to the application, the data subject applied to the Personal Data Protection Authority, alleging that their personal data had been obtained and processed without their explicit consent after they had been contacted to arrange an appointment in connection with insurance services. The applicant company, however, argued that the data subject's name, surname, and telephone number had been obtained from a website, that the data had been made public by the data subject, and that they could therefore be processed without explicit consent pursuant to Article 5(2)(d) of Law No. 6698 on the Protection of Personal Data.

The Personal Data Protection Board concluded that, even if the data in question had been available on the website, the company had not used them in a manner consistent with the purpose for which they had been made public. Accordingly, the Board imposed an administrative fine on the grounds that the necessary technical and organisational measures had not been taken to prevent the unlawful processing of personal data.

In its assessment, the Constitutional Court noted that names, surnames, and telephone numbers constitute personal data and that, as a general rule, personal data may not be processed without the explicit consent of the data subject.

However, the Court found that Law No. 6698 contains no express provision defining the purpose for which personal data are made public, regulating the use of publicly disclosed personal data for purposes incompatible with that purpose, or subjecting such use to a separate sanction.

Against this background, the Constitutional Court concluded that the imposition of an administrative fine on the basis of the concept of the "purpose for which the data were made

public”, which is not expressly regulated by law, was not foreseeable for the applicant company. The Court further found that the grounds on which the applicant had been regarded as a data controller, as well as whether the website on which the data had initially been published bore any responsibility, had not been set out with sufficient clarity.

In conclusion, the Constitutional Court held that the principle of legality of offences and penalties, which also applies to administrative sanctions, had been violated. The judgment is significant in demonstrating that, when imposing administrative sanctions under Law No. 6698 on the Protection of Personal Data, it is necessary to assess not only whether the personal data processing activity is lawful, but also whether the statutory basis of the conduct subject to the sanction is sufficiently clear, precise, and foreseeable.

The full text of the judgment is available [here](#).

3 A Noteworthy Decision of the Istanbul 14th Commercial Court of First Instance on the Enforcement of Foreign Judgments and the Use of Artificial Intelligence in Judicial Proceedings

DECISION DATE: 30.04.2026

FILE NUMBER: M. 2025/976, D. 2026/413

The dispute giving rise to the decision arose from a consultancy agreement concerning an eye clinic intended to be established in the Netherlands. Recognition and enforcement proceedings were initiated in Türkiye to render a judgment delivered by the Dutch court in favour of the claimant enforceable.

The Court assessed the conditions for enforcement under Law No. 5718 on Private International Law and International Civil Procedure. In this context, it separately examined whether the foreign judgment had become final, whether the requisite documents had been submitted, whether the Court had jurisdiction, whether the foreign claimant was required to provide security for costs, whether reciprocity existed, and whether recognition or enforcement would be contrary to public policy.

The Court held that the Commercial Court of First Instance had jurisdiction, as both parties were merchants and the dispute concerned a commercial receivable. It further concluded that, pursuant to the 1954 Hague Convention on Civil Procedure, to which both Türkiye and the Netherlands are parties, the claimant company domiciled in the Netherlands was exempt

from providing security for costs solely on the grounds of its foreign status.

The Court noted that, although no bilateral agreement on the recognition and enforcement of judgments exists between Türkiye and the Netherlands, the reciprocity requirement is not limited to treaty-based reciprocity. Having regard to the relevant provisions of Dutch law and recent judicial decisions, the Court found that both statutory and de facto reciprocity existed.

As regards the public policy objection, the Court held that the penalty clause contained in the foreign judgment was not manifestly contrary to Turkish public policy, taking into account the parties' status as merchants and the principle of freedom of contract.

Another noteworthy aspect of the decision is the Court's express acknowledgment that artificial intelligence was used as an auxiliary technical tool during the preparation of the judgment to verify sources of foreign law and assist with translation.

Ultimately, the Court decided to enforce certain provisions of the Dutch court judgment and to recognise others. The decision is significant both for its interpretation of the reciprocity requirement between Türkiye and the Netherlands and for its acknowledgement of artificial intelligence as an auxiliary technical tool in judicial proceedings.

The full text of the judgment is available [here](#).

4 Constitutional Court Annulment Decision Concerning E-Commerce Intermediary Service Providers

DECISION DATE: 12.02.2026

The Constitutional Court held that granting intermediary service providers a complete exemption from liability for consumer claims arising from defective goods, and establishing a general regime of non-liability in relation to consumer contracts, was incompatible with the constitutional principle of consumer protection. The annulled provisions will cease to have effect on 2 March 2027.

Although the decision does not mean that e-commerce platforms will, in all circumstances, be held liable as sellers or suppliers, it establishes that such platforms cannot benefit from an absolute and categorical exemption from liability. In assessing liability, factors such as the platform's role in the transaction, its level of knowledge of and control over the relevant goods or services, the degree of trust it creates

among consumers, and its involvement in payment, delivery, return, and complaint-handling processes may be taken into account.

The full text of the decision is available [here](#).

5 Significant Constitutional Court Judgment on Digital Evidence and Personal Data Protection

DECISION DATE: 12.02.2026



In its judgment dated 12 February 2026, the Constitutional Court annulled Article 134 of the Code of Criminal Procedure, which governs searches, copying, and seizure of computers, computer programs, and computer records, on the grounds that it was unconstitutional. The Court emphasised that digital materials may contain personal data of an exceptionally broad scope and that measures involving their search, copying, and seizure constitute an interference with the rights to respect for private life and to the protection of personal data.

The Court stated that, in the process of obtaining digital evidence, clear statutory safeguards must govern not only access to the evidence itself, but also the scope of the data accessed, the applicable retention periods, the destruction of the data, the segregation of irrelevant data, and data security. This approach is also consistent with the principles of purpose limitation, proportionality, data minimisation, and the retention of personal data only for as long as necessary under Law No. 6698 on the Protection of Personal Data. Although the judgment was not rendered by the Personal Data Protection Board directly under Law No. 6698 on the Protection of Personal Data, it highlights the importance of legality, proportionality, and effective statutory safeguards in relation to interferences with digital data in criminal proceedings. In this respect, the judgment constitutes significant case law concerning both the acquisition of digital evidence and the protection of personal data.

The full text of the judgment is available [here](#).

— GLOBAL DEVELOPMENTS

1 Türkiye Announces Its Artificial Intelligence Action Plan



The Türkiye Artificial Intelligence Action Plan, which sets out Türkiye's strategic roadmap for artificial intelligence, was unveiled at the Türkiye Artificial Intelligence Summit held in Istanbul with the participation of President Recep Tayyip Erdoğan. The Action Plan is structured around four key pillars: “recognise, harness, develop, and govern”.

Under the Action Plan, Türkiye aims to launch the National Artificial Intelligence Literacy Programme, establish AI literacy workshops across all 81 provinces, and provide training to five million citizens within two years. It also envisages the training of 10,000 advanced AI specialists and 100,000 AI implementation professionals, as well as making at least 2,000 public-sector datasets available through the National Data Library, particularly in the fields of healthcare, agriculture, defence, and e-commerce.

The Action Plan also sets out significant targets relating to data centre infrastructure and domestic AI technologies. In this context, Türkiye plans to increase its installed data centre capacity to at least 1 gigawatt by 2030, mobilise at least USD 10 billion in investment, predominantly from the private sector, in data center, cloud, and AI infrastructure, and support the development of Turkish-language large language models.

The Action Plan further provides for the establishment of a regulatory framework that protects users' rights, ensures predictability for investors, and adopts a proportionate, risk-based approach.

The full text of the announcement is available [here](#).

2 Spain Approves Draft Law Implementing the EU Artificial Intelligence Act

The Spanish Council of Ministers has approved the Draft Organic Law on the Proper Use and Governance of Artificial Intelligence, and submitted it to Parliament. The Draft Law is intended to implement the EU Artificial Intelligence Act (“AI Act”, Regulation (EU) 2024/1689) at the national level. In line with the

AI Act, it seeks to give effect under Spanish law to key safeguards concerning the risk-based classification of AI systems, the sanctions regime, human oversight, algorithmic transparency, the protection of children, and data privacy.

In certain respects, the Draft Law adopts an approach that goes beyond the current text of the AI Act. Although political agreement on these approaches was reached at EU level on 7 May 2026, the relevant amendments have not yet been formally incorporated into the AI Act. In this respect, Spain has incorporated into its national legislation an approach that it played a leading role in developing.

The Draft Law also introduces additional obligations for the central government that go beyond those laid down in the AI Act. While the AI Act requires public authorities to conduct fundamental rights impact assessments in relation to high-risk systems, the Spanish Draft Law provides for the appointment of an “AI officer” responsible for coordinating regulatory compliance within public authorities and advising on public-sector projects and procurement procedures. It also introduces a broader inventory obligation covering all AI systems used in administrative processes.

The full text of the La Moncloa announcement is available [here](#).

3 European Parliament Adopts Regulation Revising the AI Act Compliance Timeline

On 16 June 2026, the European Parliament adopted, by 423 votes in favour, 57 votes against, and 174 abstentions, the Digital Omnibus regulation amending the EU Artificial Intelligence Act (“AI Act”). The regulation postpones the application dates of certain obligations relating to high-risk AI systems, clarifies the timetable for labelling AI-generated content, and introduces an express prohibition on AI systems that generate intimate or sexual content without consent. For the regulation to enter into force, it must also be formally adopted by the Council of the European Union.

Under the revised timetable, the obligations requiring AI-generated content to be labelled in a machine-readable format will apply from 2 December 2026 to systems placed on the market before 2 August 2026. From the same date, AI

systems that generate child sexual abuse material, or images, videos, or audio depicting identifiable individuals in intimate or sexual contexts without their consent, will also be prohibited.

The application date of the obligations relating to high-risk AI systems has been postponed to 2 December 2027 for stand-alone high-risk AI systems, and to 2 August 2028 for AI systems integrated as safety components into products governed by EU sectoral product-safety legislation.

The regulation also introduces amendments aimed at reducing overlapping obligations applicable to machinery products, clarifying the concept of a “safety component”, permitting the processing of personal data—subject to appropriate safeguards—for the detection and correction of bias, extending SME-related simplifications to small and medium-sized companies, and streamlining the enforcement role of the EU AI Office in relation to certain general-purpose AI systems.

The full text of the European Parliament’s announcement is available [here](#).

4 Germany Designates the Bundesnetzagentur as the Competent Authority under the EU Data Act



Following the entry into force of the Data Act Implementation and Enforcement Act (“DADG”), the Bundesnetzagentur became the competent authority responsible for enforcing the EU Data Act in Germany on 30 May 2026. The agency will serve as the single point of contact for all matters relating to the Data Act, support market participants, and monitor compliance with its requirements.

The Bundesnetzagentur’s new responsibilities include cooperating, at both national and cross-border levels, with the Federal Commissioner for Data Protection and Freedom of Information on data protection matters, as well as with the European Commission and the European Data Innovation Board.

The agency will also certify dispute settlement bodies in Germany, monitor technological and economic developments in the data economy, contribute to standardisation initiatives aimed at enhancing data interoperability, and supervise compliance with the rules facilitating switching between cloud service providers.

The EU Data Act seeks to give consumers and businesses greater control over access to and

use of data generated by connected products, including connected vehicles, smart home devices, and industrial machinery. The Regulation applies across a wide range of sectors, including the automotive, machinery, agriculture, and healthcare sectors. It also contains provisions governing the making available of data to public-sector bodies in cases of exceptional need and facilitating switching between cloud service providers.

The full text of the Bundesnetzagentur announcement is available [here](#).

5 European Commission Publishes Code of Practice on the Labelling of AI-Generated Content

On 10 June 2026, the European Commission published the final Code of Practice on the marking and labelling of AI-generated content. The voluntary Code sets out practical measures to assist providers and deployers of generative AI systems in complying with the transparency obligations laid down in the EU Artificial Intelligence Act (“AI Act”), which will become applicable on 2 August 2026.

Under the AI Act, deepfake content and AI-generated or AI-manipulated text published on matters of public interest must be clearly labelled. Users must also be informed when they are interacting with AI systems such as chatbots. These obligations are intended to mitigate the risks of deception, manipulation, and disinformation.

The full text of the European Commission’s announcement is available [here](#).

6 European Commission Fines Temu EUR 200 Million under the DSA



On 28 May 2026, the European Commission announced that it had imposed an administrative fine of EUR 200 million on Temu for breaching its risk assessment obligations under the Digital Services Act (“DSA”). The Commission found that Temu had failed adequately to identify, analyse, and assess the systemic risks arising from the sale of illegal products on its platform.

According to the Commission, Temu’s 2024 risk assessment relied on general risks associated with the e-commerce sector rather than on service-specific data relating to its own platform. It underestimated the likelihood of consumers in the EU being exposed to illegal products and failed adequately to

assess how recommender systems and influencer-driven product promotions could amplify those risks. Testing conducted during the investigation also revealed that certain chargers and toys intended for infants did not comply with essential product safety requirements.

Pursuant to Article 75 of the DSA, Temu is required to submit, by 28 August 2026, an action plan setting out the measures it will take to remedy the infringement. If non-compliance persists, the company may be subject to periodic penalty payments.

The decision demonstrates the increasing intensity of regulatory scrutiny of online marketplaces in the areas of product safety, consumer protection, algorithmic recommender systems, and platform governance.

The full text of the European Commission's announcement is available [here](#).

7 European Parliamentary Research Service Briefing on the Debate over a Minimum Age for Social Media Use

In its June 2026 briefing, the European Parliamentary Research Service (“EPRS”) examined the ongoing debate concerning the introduction of a minimum age requirement for children's access to social media. Referring to UNICEF data, the briefing notes that age-based restrictions on access to social media are currently being debated, proposed, or implemented in approximately 40 countries. However, the experience in Australia—where many children have continued to access social media platforms despite the closure of their accounts—indicates that such restrictions may not, in themselves, constitute an effective solution.

The EPRS emphasises that age verification and age estimation technologies lie at the heart of the debate concerning a minimum age for social media use. Although these technologies are regarded as important tools for protecting children online, they also give rise to risks relating to privacy, wrongful exclusion, discrimination, the processing of biometric data, and circumvention.

Accordingly, discussions at EU level are focusing on the development of a common age-assurance framework that is privacy-preserving, proportionate, reliable, and non-discriminatory, rather than on fragmented national rules.

The briefing further notes that existing EU law does not prescribe a uniform minimum age for social media use. Nevertheless, the General Data Protection Regulation (“GDPR”), the

Digital Services Act (“DSA”), the European Digital Identity Framework, and the Audiovisual Media Services Directive play an important role in protecting children online.

From the perspective of Law No. 6698 on the Protection of Personal Data, the processing of children's personal data through age-assurance systems should be carefully assessed in light of the principles of purpose limitation, data minimisation, proportionality, transparency, and data security.

The full text of the EPRS briefing is available [here](#).

8 UK Information Commissioner's Office (“ICO”) Warns against Unauthorised Access to Patient Data in the Healthcare Sector



In its article entitled “Curiosity Is Not an Excuse: Protecting Patient Data in Healthcare”, published on 22 June 2026, the UK Information

Commissioner's Office (“ICO”) drew attention to the risk of unauthorised access to patient records in the healthcare sector. The ICO emphasised that the fact that healthcare professionals are technically able to access patient records in the course of their duties does not entitle them to review such records in all circumstances. Any access must be lawful, necessary, and directly related to the performance of their duties.

According to the ICO, the risk of healthcare professionals accessing individuals' medical records out of curiosity may increase following incidents that attract significant public attention, serious criminal cases, or matters of heightened public sensitivity. Such access is unlawful and may result in serious consequences, including disciplinary sanctions, loss of professional registration, and, in certain cases, criminal proceedings.

This assessment is also relevant from the perspective of Law No. 6698 on the Protection of Personal Data. Health data constitute special categories of personal data under Article 6 of Law No. 6698. Accordingly, such data may be processed and accessed only where an applicable legal ground exists and only to the extent necessary for a specified duty, authority, and purpose. The mere existence of technical access privileges does not, in itself, confer a legal right of access.

Under Article 12 of Law No. 6698, data controllers should provide their employees with data

protection training supported by practical examples to help ensure that personal data are processed lawfully and accessed only by authorised personnel for legitimate purposes.

The ICO further noted that, following incidents attracting public attention, an immediate reminder from senior management regarding patient confidentiality and data protection obligations may constitute an effective preventive measure. This approach demonstrates that a strong data security culture within healthcare organisations should be supported not only by technical controls, but also by robust institutional awareness, accountability, and regular oversight.

In conclusion, the ICO's statement makes clear that the decisive criterion for access to health data is not whether an individual is technically able to access such data, but whether the access is necessary for the performance of their duties and is legally justified. Given that health data constitute special categories of personal data, healthcare organisations must manage access to patient records in accordance with the principles of least privilege, purpose limitation, and regular oversight.

The full text of the ICO's article is available [here](#).

9 CNIL Guidance on GDPR Roles and Responsibilities in Cloud Computing Services



On 28 May 2026, the French Data Protection Authority (“CNIL”) published guidance on determining the respective roles of parties under the GDPR in the context of cloud computing services. The guidance emphasises that the proper classification of parties as controllers, joint controllers, or processors within the cloud computing ecosystem is essential for determining their contractual obligations, implementing appropriate data security measures, and facilitating the exercise of data subjects' rights.

According to CNIL, the parties' respective roles in relation to cloud services must be determined on a case-by-case basis. This assessment should take into account the differing levels of control inherent in Infrastructure as a Service (“IaaS”), Platform as a Service (“PaaS”), and Software as a Service (“SaaS”) models, the customer's ability to configure the service, and the service provider's actual influence over the relevant processing operations.

As a general rule, a customer that uses a cloud service for its own purposes will be regarded

as the data controller, while a cloud service provider that processes personal data on the customer's documented instructions will be regarded as the data processor. However, where the provider determines its own purposes and means of processing, including in connection with service improvement activities, monitoring tools, or cookies, it may be classified as an independent controller or, where the purposes and means are jointly determined with another party, as a joint controller.

The guidance is also relevant from the perspective of Law No. 6698 on the Protection of Personal Data. The allocation of roles and responsibilities between cloud service customers and service providers should be clearly defined at both contractual and operational levels. In this context, matters such as the purposes and scope of processing, the customer's instructions, data security measures, the engagement of sub-processors, data retention and destruction procedures, access rights, and the handling of data subject requests should be clearly regulated.

The full text of the CNIL guidance is available [here](#).

10 Ten Guiding Principles from the UN Human Rights Office on Children's Online Safety

The Office of the United Nations High Commissioner for Human Rights (“OHCHR”) has published guidelines entitled “Getting Children's Safety Online Right” setting out ten guiding principles for protecting children in the online environment.

The guidelines state that children's online safety cannot be ensured solely through access bans or general restrictions on social media use. Instead, they recommend that online platforms adopt a safety-by-design approach, address addictive design features, strictly regulate online marketing directed at children, and prevent children from being subjected to commercial micro-targeting. They further state that companies should conduct child rights impact assessments and that platforms should be subject to transparency reporting obligations concerning their impact on children.

The OHCHR draws attention to the need for robust privacy and data protection safeguards where age assurance systems are used. In this context, it recommends limiting the collection and retention of personal data, ensuring transparency regarding age assurance providers,

assessing the risk of discrimination, and developing accessible solutions for children who do not possess official identification documents.

The guidance further states that age-based restrictions should not be imposed in a generalised manner but should instead be targeted at specifically identified harms.

The relevant article is available [here](#).

11 German Court Ruling on Google's Liability for AI Overviews

DECISION DATE: 27.01.2026



The Munich Regional Court issued a noteworthy ruling finding that Google may be held liable for inaccurate statements generated through its AI Overviews feature. The Court held that Google is required to prevent the dissemination of misleading or factually incorrect AI-generated statements in its search results.

The dispute arose from AI-generated summaries that associated certain publishing companies with questionable commercial practices and allegations of fraud without any substantiated basis. The Court noted that, unlike a traditional search engine, AI Overviews does not merely display or link to third-party content, but generates new and independent statements based on existing sources.

The decision is significant in demonstrating that companies that design, train, operate, and manage AI systems may be held liable for harm caused by inaccurate content generated by those systems. It further indicates that, in the context of generative AI systems, a general disclaimer stating that outputs may be inaccurate may not, in itself, be sufficient to exclude liability.

The full text of the WIRED article is available [here](#).

12 Austrian Data Protection Authority Decision on the Mandatory Selection of a Gender-Based Form of Address

DECISION DATE: 24.11.2025

FILE NUMBER: 2025-0.950.759

In the case giving rise to the complaint, the data subject was required to select a gendered form of address when creating an account with an online store. The data subject subsequently requested that the data controller cease using

gender-specific forms of address in communications addressed to them. The data controller initially stated that the necessary technical modification was not possible; however, during the course of the proceedings, it updated its system to enable gender-neutral registration.



Although the Austrian Data Protection Authority (“**DSB**”) found that the infringement had been remedied in relation to the data subject’s requests for rectification and erasure, it separately examined whether the previous processing activity had complied with the principles set out in Article 5 of the GDPR.

Referring also to the judgment of the Court of Justice of the European Union in Case C-394/23, *Mousse*, the DSB found that data relating to a gendered form of address were not necessary for the performance of the contract and that processing such data for personalised commercial communications was incompatible with the principle of data minimisation. In particular, the DSB concluded that such processing was not necessary for order processing, delivery, payment, or commercial communications, especially where less intrusive and equally effective alternatives were available.

The decision further states that the data controller could rely neither on the legal basis of performance of a contract under Article 6(1)(b) of the GDPR nor on legitimate interests under Article 6(1)(f). According to the DSB, although an economic interest in addressing customers in a personalised manner may, in principle, constitute a legitimate interest, the mandatory processing of data relating to a gendered form of address was not necessary in the circumstances of the case.

The DSB therefore found that the processing activity was contrary to the principles of purpose limitation under Article 5(1)(b) and data minimisation under Article 5(1)(c) of the GDPR.

The full text of the decision is available [here](#).

13 Ministry of Justice Announces a New Era of AI-Assisted Judicial Services

The Ministry of Justice has announced a new era of AI-assisted judicial services through the UYAP AI Decision Support System, which is intended to enhance the speed, efficiency, and effectiveness of judicial proceedings. The system is designed to assist judges and public prosecutors in areas such as searching case law and precedent, summarising case files, preparing draft reasoned judgments, analysing evidence, and evaluating expert reports.

The announcement emphasises that the system will not act as an autonomous decision-maker, but solely as a decision-support tool. Final decisions will remain the responsibility of judges and public prosecutors, and the relevant processes will be conducted under human oversight in a transparent and auditable manner.

The full text of the announcement is available [here](#).

14 World Economic Forum Assessment of the Human Factor in AI Adoption

The World Economic Forum emphasised that the successful adoption of AI in the workplace depends not only on technological infrastructure, but also on employee trust, psychological readiness, and organisational culture. The article noted that employees approach AI with varying degrees of openness and that concerns such as job displacement, workplace surveillance, loss of skills, and distrust of technology may affect the adoption process.

Accordingly, organisations should manage AI adoption not only through technical training, but also through human-centred strategies that take employees' concerns and expectations and levels of readiness into account.

The full text of the WEF article is available [here](#).

15 Independent Expert Report Commissioned by the European Commission on the Societal Impacts of Artificial Intelligence

The report, prepared by independent experts commissioned by the European Commission's Directorate-General for Research and Innovation, emphasises that AI offers significant opportunities in areas including healthcare, climate resilience, productivity, and sustainability. However, it also stresses that these opportunities should be assessed within a governance framework aligned with the principles of equality, transparency, accountability, and human dignity.

The report further draws attention to risks and challenges including a lack of transparency, disinformation, inequalities in access to resources, the protection of personal data, AI-enabled workplace surveillance, and intellectual property rights. It states that human oversight, privacy, accountability, and societal impact as-

sessments should be addressed in an integrated manner throughout the development and deployment of AI systems.

The full text of the report is available [here](#).

16 European Data Protection Supervisor Warns of Data Protection and Security Risks Arising from Shadow AI

The European Data Protection Supervisor ("EDPS") defines "shadow AI" as employees' use of generative AI chatbots, coding assistants, automated meeting-recording tools, or similar AI systems without institutional approval. The EDPS warns that such use may give rise to significant data protection and information security risks. In particular, organisations may lose visibility and control over where data entered into unauthorised AI tools are stored, who may access them, how long they are retained, and whether they are used for model training. From the perspective of Law No. 6698 on the Protection of Personal Data, the use of unauthorised AI tools should be carefully assessed in light of the principles of purpose limitation, data minimisation, lawful processing, and data security. Data controllers should not rely solely on general warnings. Instead, they should clearly specify which AI tools are approved for use, the purposes for which such tools may be used, and the categories of data that must not be entered into them. The EDPS identifies clear AI use policies, data classification rules, access controls, employee awareness and training, and the provision of secure and institutionally approved alternatives as key safeguards against the risks associated with shadow AI. The full text of the EDPS blog post on this matter is available [here](#).

CONTACT

EGE ÇAKIRCA ATTORNEYS AT LAW



Esentepe Mahallesi Harman 1 Sokak Harmancı Giz Plaza No: 5 Kat: 5 – İstanbul 34394



info@eclawtr.com



+90 212 352 3318



eclawtr.com



EGE • ÇAKIRCA



Founding Partner
Özlem EGE POLAT



Associate
Ceren AYDEMİR



Legal Trainee
Ezgi OPRUKÇU