

EGE ÇAKIRCA

Attorneys at Law

DATA PROTECTION BULLETIN

August 2026



**JUDICIAL
DECISIONS**



**DEVELOPMENTS
IN TÜRKİYE**



**GLOBAL
DEVELOPMENTS**



August 2026 witnessed significant developments in data protection law, particularly in relation to data breaches, the use of biometric data, data subjects' right of access, transparency and explicit consent obligations, direct marketing activities, automated decision-making systems, the protection of children's personal data, and the processing of employee data.

This newsletter covers decisions and data breach announcements published by the Turkish Personal Data Protection Board ("**Board**"), as well as the Principle Decision on loyalty cards, the Türkiye Artificial Intelligence Action Plan, significant international judicial decisions in the fields of artificial intelligence, data protection and digital law, and recent developments in Europe concerning employee data, automated decision-making processes and the protection of children's personal data under the General Data Protection Regulation ("**GDPR**").



JUDICIAL DECISIONS

- Amazon v. Perplexity AI Decision on Unauthorized Access in the Use of Agentic AI
- Justice et al. v. Suno, Inc. Decision on the Use of Copyrighted Works in Training Generative AI Models
- UK Upper Tribunal Decision on the Processing of Children's Personal Data on TikTok
- Danish Supreme Court Decision on Compensation for Unlawful Data Transfers

TR DEVELOPMENTS in TÜRKİYE

- !! Data Breach Announcements Concerning Hyundai Motor Türkiye, Mega Enerji, Tamer Tanca, Çorum Municipality, Uludağ Elektrik, Travelport and WestJet, Among Others
- !! Guidelines on the Protection of Personal Data in the Use of Smart Glasses
- !! Assessment of Fingerprint-Based Attendance Tracking at a University under the Principle of Proportionality
- !! Board Decisions on Bank Employees' Right of Access to Telephone Call Recordings and on Security Cameras, Transparency Obligations and Cookie Practices
- !! Board Decisions on Data Breaches at a Pharmaceutical and Healthcare Products Company and a Cosmetics and Personal Care Company
- !! Board Decision on the Explicit Consent Requirement for In-Flight Internet Services
- !! TRY 1,000,000 Administrative Fine for a Data Breach at a Restaurant and Quick-Service Chain
- !! TRY 1,000,000 Administrative Fine for Unsolicited Advertising SMS Messages and Calls
- !! Data Breach Decision Concerning a Manufacturer of Plastic Household Goods and Cleaning Products
- !! Extension of the Compliance Period until 28 February 2027 Regarding Loyalty Cards and the Use of Telephone Numbers by Third Parties
- !! Public Announcement on the Processing of Biometric Data for Employee Attendance Tracking
- !! Türkiye Artificial Intelligence Action Plan 2026–2030
- !! Preliminary Report on the Pharmaceutical Sector Inquiry Published by the Turkish Competition Authority



GLOBAL DEVELOPMENTS

- ICO Enforcement Decision Against the Metropolitan Police Service Concerning Sensitive Personal Data Breaches
- Decision of the Spanish Data Protection Authority on Digital Invoicing and Consent for Commercial Communications
- EUR 460,000 Administrative Fine Imposed on Piaggio by the Italian Data Protection Authority for the Retention and Review of Employee Emails
- Decision of the Dutch Data Protection Authority Concerning Uber's Deactivation of Driver Accounts Through Fully Automated Decision-Making
- Total GDPR Fines in Europe Reach EUR 6.31 Billion According to GDPR Enforcement Tracker Data
- Transparency and AI Content Labelling Obligations under the EU Artificial Intelligence Act
- Decision of the Brazilian Data Protection Authority Concerning Children's Personal Data Processed by TikTok/ByteDance



This bulletin, prepared by Ege akırca Attorneys at Law in relation to legal developments concerning personal data protection law and artificial intelligence law during August 2026, is intended solely for general informational purposes and does not constitute legal advice, a legal opinion, or consultancy services of any kind. As the content has not been prepared for application to any specific matter, it does not create 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.

JUDICIAL DECISIONS

1 Amazon v. Perplexity AI Decision on Unauthorized Access in the Use of Agentic AI



DECISION NO: 26-144

PUBLICATION DATE: 04.08.2026

The U.S. Court of Appeals for the Ninth Circuit (“**Court**”) vacated the preliminary injunction that had prohibited the use of Perplexity’s AI agent integrated into the Comet browser on Amazon.com in *Amazon.com Services, LLC v. Perplexity AI, Inc.*

The dispute arose from an AI agent called “Assistant,” which carried out product searches and shopping transactions on Amazon in accordance with user instructions.

The Court considered Amazon unlikely to succeed on the merits of its claims under the federal Computer Fraud and Abuse Act (“**CFAA**”) and the California Comprehensive Computer Data Access and Fraud Act (“**CDAFA**”). Ac-

cording to the Court, the party accessing Amazon’s systems was not Perplexity itself, but rather the user employing Assistant as a tool. The Court further found that Perplexity’s processing of screenshots and transmission of instructions to the agent did not, by themselves, constitute “access.”



While the decision is notable in terms of whether the actions of AI agents should be attributed to the user or to the service provider, the Court’s assessment remained limited to the technical architecture of the specific case and the meaning of “access” under the CFAA and CDAFA.

You can access the full text of the decision [here](#).

2 Justice et al. v. Suno, Inc. Decision



DECISION NO: 25-11739-FDS

PUBLICATION DATE: 20.08.2026

The U.S. District Court for the District of Massachusetts (“**Court**”) largely denied Suno, Inc.’s motion to dismiss in a lawsuit brought by independent musicians against the generative artificial intelligence company. The plaintiffs alleged that their copyrighted songs had been copied from YouTube and used to train Suno’s model, and that Suno was capable of generating outputs identical or substantially similar to those works.

Although the plaintiffs had not yet identified specific outputs that were substantially similar to their own works, the Court found their factual allegations that the model could imitate or reproduce existing works sufficient, at this stage of the proceedings, to allow their claim based

on the derivative works right to proceed. The Court also held that the allegation that YouTube’s technical access restrictions had been circumvented could be examined under the Digital Millennium Copyright Act (“**DMCA**”). By contrast, the claim brought under the Tennessee Consumer Protection Act was dismissed.



The decision is notable for illustrating the circumstances in which claims concerning the use of copyrighted works in the training of generative AI models and the similarity of model outputs to such works may survive at an early stage of litigation.

You can access the full text of the decision [here](#).

3 UK Upper Tribunal Decision on the Processing of Children’s Personal Data on TikTok



DECISION DATE: 28.07.2026

PUBLICATION DATE: 04.08.2026

The UK Upper Tribunal (“**Upper Tribunal**”) rejected TikTok’s preliminary objection in its appeal against the GBP 12.7 million administrative fine imposed

for infringements relating to the processing of personal data of children under the age of 13.

The Upper Tribunal held that the processing activities subject to the fine could not be

regarded as processing carried out for journalistic, academic, artistic or literary “**special purposes**” within the meaning of the Data Protection Act 2018.

Accordingly, the Upper Tribunal concluded that the additional procedural preconditions relied on by TikTok were not required in order for the Information Commissioner to impose the fine.



The decision also noted that the infringements of Articles 5(1)(a) and 8 of the UK GDPR concerned

the processing of personal data of children below the applicable age threshold, while the infringements of Articles 12 and 13 concerned transparency and information obligations.

The case was remitted to the UK First-tier Tribunal (“**First-tier Tribunal**”) for consideration of the remaining issues that had not yet been determined.

You can access the full text of the decision [here](#).

4 Danish Supreme Court Decision on Compensation for Unlawful Data Transfers

DECISION DATE: 24.08.2026

The Danish Supreme Court (“**Court**”) held, in a case concerning the accidental disclosure by a municipality of an individual’s mental health information to a third party, that the transfer violated data protection rules and the right to respect for private life.



The Court concluded that the individual had suffered non-material damage, taking into account the highly sensitive nature of the information disclosed, the fact that it had been transferred to a person with whom the individual

was in dispute, and that it was subsequently forwarded to another institution.

Accordingly, the Supreme Court increased the amount of compensation previously awarded by the Eastern High Court from DKK 2,500 to DKK 30,000.



The decision is significant in terms of compensation for non-material damage arising from data protection infringements.

You can access the full text of the decision [here](#).

DEVELOPMENTS IN TURKIYE

1 Public Announcement on the Data Breach Notification of Hyundai Motor Türkiye Otomotiv A.Ş.



RELEASE DATE: 05.08.2026

The Turkish Personal Data Protection Authority (“**Authority**”) announced a data breach concerning Hyundai Motor Türkiye Otomotiv A.Ş.

The breach reportedly occurred as a result of the exploitation of an SQL injection vulnerability in the company’s web application and affected the personal data of employees and job applicants, including names and surnames, email addresses, personality

inventory results, usernames, passwords and job titles.



It was stated that up to 422 individuals may have been affected by the breach. Data subjects affected by the breach may contact the data controller via “info@hyundai.com.tr” and “dpo@hyundai.com.tr” to obtain further information.

You can access the full text of the announcement [here](#).

2 Public Announcement on the Data Breach Notification of Mega Enerji Güç Sistemleri A.Ş.



RELEASE DATE: 05.08.2026

The Turkish Personal Data Protection Authority (“**Authority**”) published the data breach notification submitted by Mega Enerji Güç Sistemleri A.Ş.

It was reported that the breach was detected on 25 July 2026 and that the company’s central information technology, storage and backup systems had been encrypted and rendered inaccessible.

The breach affected various categories of personal data, including identity, contact, financial, personnel, transaction security and customer transaction data. The affected groups included employees, users, students, customers and prospective customers. The number of affected individuals has not yet been determined.

You can access the full text of the announcement [here](#).

3 Public Announcement on the Data Breach Notification of Tamer Tanca Mağazacılık Sanayi ve Ticaret A.Ş.



RELEASE DATE: 05.08.2026

The Turkish Personal Data Protection Authority (“**Authority**”) published the data breach notification submitted by Tamer Tanca Mağazacılık Sanayi ve Ticaret A.Ş.

It was reported that the breach resulted from a cyberattack, although the method of attack has not yet been identified. The incident came to light after a customer’s personal data was used in an attempted fraud.



The data believed to have been compromised included customer names, contact information and order details. Customers and prospective customers were identified as the affected groups. While the exact number of affected individuals could not be determined, it was stated that the number may be as high as 50,000.

You can access the full text of the announcement [here](#).

4 Guidelines on the Protection of Personal Data in the Use of Smart Glasses

RELEASE DATE: 28.08.2026



The Turkish Personal Data Protection Authority (“**Authority**”) published guidelines on the protection of personal data and privacy in the use of smart glasses, which are capable of processing various types of data such as images, audio, location, date, time and usage information.

The Authority emphasized that the scope and duration of recordings should be limited to what is necessary, that particular care should be exercised with respect to audio recordings, and that recording features should not be used in environments where there is a heightened expectation of privacy.



The guidelines also recommend conducting an appropriate assessment before sharing images containing other individuals and, where necessary, obtaining their consent, deleting recordings that are no longer needed, and regularly reviewing the privacy and security settings of the devices.

The Authority further noted that recording or sharing images or audio may, depending on the circumstances of the specific case, give rise to civil or criminal liability.

You can access the guidelines published on 28 August 2026 [here](#).

5 Board Decision on Fingerprint-Based Attendance Tracking at a University

DECISION DATE: 08.02.2024

DECISION NO: 2024/197

RELEASE DATE: 10.08.2026



The Turkish Personal Data Protection Board (“**Board**”) issued a decision following a complaint and an ex officio investigation concerning the use of fingerprint data to monitor students’ class attendance at a university.



The Board considered fingerprint data to constitute biometric data and therefore special categories of personal data. It further held that processing such data for attendance tracking purposes was contrary to the principle of proportionality, even where the students had provided explicit consent.

Accordingly, the Board decided that the biometric attendance tracking practice should be discontinued, the existing fingerprint data should be destroyed, and student attendance should instead be monitored through alternative methods that do not require the processing of biometric data. The data controller was also instructed to inform the Board of the actions taken in this respect.

You can access the full text of the decision [here](#).

6 Board Decision on a Bank Employee’s Request for Access to Call Recordings

DECISION DATE: 18.04.2024

DECISION NO: 2024/592

RELEASE DATE: 10.08.2026



The Turkish Personal Data Protection Board (“**Board**”) evaluated an application concerning a bank employee’s request for access to the recording of a telephone conversation with a customer, which had been rejected by the bank.

The Board stated that the right of access to personal data under Article 11 of the Law also includes the data subject’s right to access his

or her own personal data, and that the presence of confidential customer information does not entirely eliminate this right.



Accordingly, the Board decided that, in order to enable the bank employee to pursue legal remedies, the call recording should be provided to the employee either in written transcript form or in digital format, with any banking data constituting third-party customer secrets appropriately redacted.

The Board also reiterated that data subject requests must be assessed effectively and in compliance with the law and the principle of good faith.

You can access the full text of the decision [here](#).

7 Board Decision on Security Cameras, Transparency Obligations and Cookie Practices



DECISION DATE: 08.08.2024

DECISION NO: 2024/1361

RELEASE DATE: 10.08.2026

The Turkish Personal Data Protection Board (“**Board**”) assessed a data controller’s use of security cameras, cookie practices on its website, compliance with transparency obligations, and explicit consent mechanisms for advertising and marketing purposes.

The Board found the recording of images only through security cameras to be lawful. However, it considered the activation of analytics cookies requiring explicit consent without obtaining prior user consent, as well as

the failure to duly fulfil the transparency obligation, to be unlawful.



The Board further stated that a request for information about a service cannot be made conditional upon giving explicit consent for advertising and marketing purposes, and that explicit consents relating to different processing purposes must be obtained separately.

You can access the full text of the decision [here](#).

8 Board Decision on a Data Breach at a Restaurant and Quick-Service Chain

DECISION DATE: 09.01.2025

DECISION NO: 2025/88

RELEASE DATE: 10.08.2026

The Turkish Personal Data Protection Board (“**Board**”) assessed a data breach that occurred at a restaurant chain and quick-service food company.

The Board found that the breach occurred after the username and password credentials stored in an IT employee’s browser were compromised through malware. The incident affected the personal data of 505,337 customers, including names and surnames, gender, email addresses, telephone numbers and city information.



The Board concluded that, prior to the breach, two-factor authentication, monitoring and alert

mechanisms, and employee training had not implemented at an adequate level, and that the necessary technical and administrative measures required under Law No. 6698 on the Protection of Personal Data (“**Law**”) had not been taken.

Accordingly, the Board imposed an administrative fine of TRY 800,000 on the data controller and an additional TRY 200,000 fine for failing to notify the affected data subjects in a timely manner, bringing the total administrative fine to TRY 1,000,000.

You can access the full text of the decision [here](#).

9 Board Decision on Unsolicited SMS Messages and Calls by a Savings Finance Company



DECISION DATE: 10.06.2026

DECISION NO: 2026/1183

RELEASE DATE: 10.08.2026

The Turkish Personal Data Protection Board (“**Board**”) assessed the use by a savings finance company of telephone numbers obtained from third parties under its “brand ambassador” program for advertising and marketing purposes.



The Board stated that, where a data subject’s telephone number had been shared by a third party, subsequent calls and SMS messages were not based on valid explicit consent within the meaning of Law No. 6698 on the Protection of Personal Data (“**Law**”). It further held that the continuation

of a telephone conversation could not be regarded as implied consent.

The Board also concluded that similar personal data processing activities carried out under the “brand ambassador” program were contrary to the Law.

Accordingly, an administrative fine of TRY **1,000,000** was imposed on the data controller.

You can access the full text of the decision [here](#).

10 Preliminary Report on the Pharmaceutical Sector Inquiry Published by the Turkish Competition Authority



RELEASE DATE: 10.08.2026

The Turkish Competition Authority (“**Authority**”) published the Preliminary Report on the Pharmaceutical Sector Inquiry (“**Preliminary Report**”) as part of its sector inquiry aimed at identifying structural competition issues in the pharmaceutical sector and developing potential solutions.



The Preliminary Report examines the overall structure of the pharmaceutical sector, the Authority’s activities over the past ten years, and competitive conditions at the production, market entry and distribution stages. It also assesses the

effects of patents and intellectual property rights, market entry conditions, exclusivity practices, public procurement of pharmaceuticals and the regulatory framework on competition.

The Authority also set out practical policy and solution proposals aimed at addressing the identified competition concerns. It further stated that public comments on the Preliminary Report may be submitted to the Authority.

You can access the Preliminary Report [here](#).

11 Board Decision on a Data Breach Concerning a Manufacturer of Plastic Household Goods and Cleaning Products



DECISION DATE: 26.12.2024

RELEASE DATE: 10.08.2026

The Turkish Personal Data Protection Board (“**Board**”) examined a ransomware attack targeting the systems of a data controller engaged in the manufacture of plastic household goods and cleaning products. As a result of the attack, the company’s data were encrypted, and it was considered possible that personal data had also been obtained by the attackers. The Board further found that the



data controller had provided inconsistent statements regarding the categories of data and individuals affected by the breach.

The investigation found that the risk assessments were inadequate, security testing had been ineffective in preventing the breach, two-factor authentication had only been implemented after the incident, and network segmentation measures were insufficient.

Accordingly, the Board imposed an administrative fine of **TRY 250,000** on the data controller for failing to implement the necessary technical and administrative measures.

You can access the full text of the decision [here](#).

12 Board Decision on a Data Breach at a Pharmaceutical and Healthcare Products Company



DECISION DATE: 07.11.2024

DECISION NO: 2024/1898

RELEASE DATE: 10.08.2026

The Turkish Personal Data Protection Board (“**Board**”) assessed a ransomware attack affecting the systems of a data controller operating in the pharmaceutical and healthcare products sector. The Board found that the breach occurred as a result of the server being encrypted through malicious software and that the attackers carried out various unauthorized activities on the system.

It was stated that **520 individuals** were affected by the breach, including 196 current employees, 303 former employees and 17 customers or business partners. The affected personal data included identity, contact, personnel and customer transaction data.



The Board concluded that the measures taken in relation to network and server security, logging, endpoint security, authorization, vulnerability scanning and penetration testing were insufficient, and that the data controller had failed to exercise the necessary care and diligence in monitoring personal data security.

Accordingly, the Board imposed an administrative fine of **TRY 350,000** on the data controller for failing to implement the necessary technical and administrative measures under Article 12 of Law No. 6698 on the Protection of Personal Data (“**Law**”).

You can access the full text of the decision [here](#).

13 Board Decision on a Data Breach at a Cosmetics and Personal Care Company



DECISION DATE: 09.10.2024

RELEASE DATE: 10.08.2026

The Turkish Personal Data Protection Board (“**Board**”) assessed a data breach that occurred at a cosmetics and personal care company.

The Board found that the breach resulted from a “Trojan” malware infection on one of the data controller’s network servers, enabling attackers to gain unauthorized access to certain personal data and demand a ransom of 45 Bitcoin.

Approximately 432 customers and business partners in Türkiye were affected. The compromised data included 325 copies of identity cards or residence permits, as well as identity and contact information relating to 107 brand ambassadors.



The Board concluded that the data controller had failed to implement adequate endpoint detection and response solutions prior to the breach, that its risk assessments were insufficient, and that security controls such as regular vulnerability scans and penetration testing had not been effectively carried out. It therefore found that the necessary technical and administrative measures required under Article 12 of Law No. 6698 on the Protection of Personal Data (“**Law**”) had not been implemented.

Accordingly, an administrative fine of TRY 500,000 was imposed on the data controller.

You can access the full text of the decision [here](#).

14 Public Announcement on the Data Breach Notification of Çorum Municipality

RELEASE DATE: 12.08.2026



The Turkish Personal Data Protection Authority (“**Authority**”) published the data breach notification submitted by Çorum Municipality.

It was reported that the breach resulted from unauthorized access to data through the municipality’s software systems and was detected on 2 August 2026.



It was alleged that third parties had copied taxpayers’ Turkish Republic identification numbers, names and surnames, mobile phone numbers and address information. Approximately 200,000 individuals were reported to have been affected by the breach.

You can access the full text of the announcement [here](#).

15 Public Announcement on the Data Breach Notification of Uludağ Elektrik Dağıtım A.Ş.

RELEASE DATE: 12.08.2026



The Turkish Personal Data Protection Authority (“**Authority**”) published the data breach notification submitted by Uludağ Elektrik Dağıtım A.Ş. (“**UEDAŞ**”).

It was stated that the breach occurred because certain third-party electricians submitting applications through the New Connection System (“**YBS**”) entered incorrect telephone numbers and/or email addresses, resulting in application-related notifications being sent to unrelated third parties.

As part of the breach, the personal data of 2,569 individuals were sent to 581 different persons, affecting a total of 3,150 individuals. The affected data included names and surnames, addresses, application information, telephone numbers and email addresses.

You can access the full text of the announcement [here](#).

16 Principle Decision on Loyalty Cards

DECISION DATE: 22.07.2026

DECISION NO: 2026/1491

PUBLICATION DATE: 13.08.2026



The Turkish Personal Data Protection Board (“**Board**”) extended the compliance period granted to data controllers under its Principle Decision dated 11 February 2026 and numbered 2026/266 concerning the use, during shopping transactions, of loyalty cards or mobile phone numbers associated with loyalty card memberships by third parties.

Under the relevant Principle Decision, data controllers had been granted a six-month period to establish mechanisms to verify that shopping transactions were carried out with the

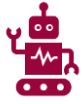
knowledge and consent of the loyalty card holder and to implement the necessary technical and administrative measures.



Taking into account requests from the sector, the Board decided to extend the compliance period, which was due to expire on 28 August 2026, until 28 February 2027.

You can access the full text of the decision [here](#).

17 Türkiye Artificial Intelligence Action Plan 2026–2030



PUBLICATION DATE: 18.08.2026

The Türkiye Artificial Intelligence Action Plan (2026–2030) was published in the Official Gazette dated 18 August 2026 through Presidential Circular No. 2026/9.

The Action Plan sets out Türkiye’s national framework for policies and practices in the field of artificial intelligence. It is also significant

from a data protection law perspective, particularly due to its potential impact on AI governance and the processing of personal data in AI systems.

You can access the full text of the Circular [here](#).

18 Public Announcement on the Data Breach Notification of Travelport International Operations Limited



RELEASE DATE: 26.08.2026

The Turkish Personal Data Protection Authority (“**Authority**”) published the data breach notification submitted by Travelport International Operations Limited.



It was reported that the breach resulted from an API configuration error in the ViewTrip application, which allowed reservation records to be viewed using only the booking reference, and

that an unauthorized third party gained limited access to the data.

The breach affected **73,958 individuals**. The affected data included passenger names, PNR and reservation information, flight, hotel, car rental and rail itinerary information and, in certain cases, contact details.

You can access the full text of the announcement [here](#).

19 Public Announcement on the Data Breach Notification of WestJet, an Alberta Partnership

RELEASE DATE: 26.08.2026

The Turkish Personal Data Protection Authority (“**Authority**”) published the data breach notification submitted by WestJet, an Alberta Partnership (“**WestJet**”).

It was reported that the breach occurred after attackers gained access to the company’s network using valid employee credentials, exfiltrated personal data, and deployed ransomware on certain systems.



The breach affected 2,774 individuals. The affected data included names and surnames, contact and identification information, passport data, reservation and PNR information, loyalty program information, and various data relating to travel requirements.

You can access the full text of the announcement [here](#).

20 Public Announcement on the Processing of Biometric Data for Employee Attendance Tracking



DECISION DATE: 29.04.2026

RELEASE DATE: 27.08.2026

The Turkish Personal Data Protection Authority (“**Authority**”) issued additional explanations on the use of biometric data in response to requests for clarification received following the Principle Decision dated 29 April 2026 and numbered



2026/921 on the Processing of Biometric Data for Employee Attendance Tracking.

The Authority emphasized that data obtained through methods such as fingerprint and palm scanning, which are capable of uniquely identifying or authenticating an individual, retain their nature as biometric data even where they

are converted into and stored as mathematical codes. It further stated that the processing of biometric data solely for the purpose of monitoring employees' working hours may fail to satisfy the principle of proportionality even where valid explicit consent has been obtained, and should be assessed in accordance with Principle Decision No. 2026/921.

However, the Authority noted that biometric data processing carried out for authentication, authorization and access control purposes in critical facilities and areas requiring a high level of security may be assessed differently from employee attendance tracking within the scope of the Principle Decision. Such processing

should nevertheless be limited to the necessary areas and individuals, used where alternative methods are insufficient, and remain proportionate to the specific security need.



The Authority also stated that the lawfulness of biometric data processing activities carried out for purposes other than employee attendance tracking must be assessed separately, taking into account the purpose of processing, the nature of the work and the specific circumstances of each case.

You can access the full text of the announcement [here](#).

21 Board Decision on the Explicit Consent Requirement for In-Flight Internet Services



DECISION DATE: 15.08.2024

RELEASE DATE: 10.08.2026

The Turkish Personal Data Protection Board ("**Board**") assessed a complaint concerning the requirement for passengers to provide explicit consent in order to use internet services offered during a flight.

The Board determined that verifying a passenger's surname together with their seat or ticket number through the airline's systems was necessary for the provision of the internet service and that such processing could rely on one of the legal grounds for processing other than explicit consent under Article 5(2) of Law No. 6698 on the Protection of Personal Data ("**Law**").

The Board also concluded that the airline and the internet service provider acted as separate data controllers in relation to this processing activity.

The Board further considered that requesting explicit consent for a processing activity that did not require such consent was misleading to the data subject and contrary to the principle of lawfulness and fairness. Accordingly, the Board imposed an administrative fine of **TRY 90,000** on the data controller internet service provider.

You can access the full text of the announcement [here](#).

GLOBAL DEVELOPMENTS

1 ICO Enforcement Action Against the MPS for Serious Personal Data Breaches



DECISION DATE: 28.07.2026

PUBLICATION DATE: 04.08.2026

The UK Information Commissioner's Office ("ICO") issued a reprimand and an enforcement notice to the Metropolitan Police Service ("MPS") following two serious personal data breaches.

In the first incident, the address and telephone number of a stalking victim, which had been changed for security reasons, together with the contact details of three witnesses, were disclosed without the necessary redactions to an individual who was subject to protective measures. In the second incident, a bulk email sent to 18 individuals in connection with the "Honeytrap" investigation placed recipients in the "To" field instead of "BCC", making their names and email addresses visible to one another and allowing their connection with a sensitive criminal investigation to be inferred.

The ICO considered that the breaches pointed to systemic shortcomings in the MPS's data protection training, internal controls, monitoring and governance processes, rather than merely isolated staff errors. In this context, the MPS was required to improve completion rates for mandatory training, strengthen the monitoring of compliance processes, and enhance its governance mechanisms.



The ICO's approach demonstrates that personal data breaches should be assessed not only in terms of individual errors, but also by reference to whether the organisation has adequate training, oversight and control mechanisms in place.

You can access the full text of the decision [here](#).

2 Decision of the Spanish Data Protection Authority on Digital Invoicing and Consent for Commercial Communications



DECISION DATE: 09.09.2024

The Spanish Data Protection Authority ("AEPD") imposed an administrative fine of EUR 20,000 on a clothing retailer for sending commercial advertising to a customer whose email address had been collected for the purpose of issuing a digital invoice, where the controller was unable to demonstrate valid consent for such processing.

The AEPD found that the data controller had failed to provide sufficient log records or other concrete evidence showing that the data

subject had consented to receiving commercial communications and therefore had not fulfilled its obligation under Article 7 of the General Data Protection Regulation ("GDPR") to demonstrate consent.



The AEPD also considered it an aggravating factor that the provision of an invoice to the customer had been made conditional upon accepting advertising communications.

You can access the full text of the decision [here](#).

3 Decision of the Italian Data Protection Authority Concerning Piaggio

DECISION DATE: 18.06.2026

The Italian Data Protection Authority ("Garante") imposed an administrative fine of EUR 460,000 on Piaggio in relation to its practices concerning employees' corporate email accounts.



The Garante found that the failure to respond in a timely manner to requests concerning former employees' email accounts, the retrospective and disproportionate access to past

correspondence, and the retention of employee emails for five years after termination of the employment relationship were contrary to the principles of purpose limitation, data minimisation and storage limitation.

The Garante also ordered that access to unlawfully collected email data be discontinued.

You can access the full text of the decision [here](#).

4 Decision of the Dutch Data Protection Authority Concerning Uber

PUBLICATION DATE: 21.08.2026



The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens* – “AP”) imposed an administrative fine of **EUR 824.99 million** on Uber for making fully automated decisions concerning drivers and for failing to provide sufficient information about those processes. This amount represents the **second-highest fine imposed under the General Data Protection Regulation (“GDPR”) to date**.

The AP found that, between 2018 and 2022, Uber monitored driver behaviour and customer ratings through software, and that certain driver accounts were temporarily or permanently deactivated without human intervention due to suspected fraud or low ratings.



The AP considered that these measures, which could result in loss of income, violated the GDPR prohibition on solely automated decision-making producing legal effects or similarly significantly affecting individuals. It also found that drivers had not been adequately informed about the relevant decision-making processes.

The investigation was initiated following complaints from 171 French drivers. As Uber’s European headquarters are located in the Netherlands, the investigation was conducted by the AP under the GDPR’s one-stop-shop mechanism in cooperation with the French Data Protection Authority (“CNIL”). Uber announced that it would appeal the decision.

You can access the announcement concerning the decision [here](#).

5 Current GDPR Enforcement Tracker Statistics

PUBLICATION DATE: 21.08.2026

According to data from the GDPR Enforcement Tracker, a total of 3,206 enforcement decisions issued by data protection authorities across the European Union and the European Economic Area are currently being tracked, with the total amount of fines reaching approximately EUR 6.31 billion.

In 2026, 160 enforcement actions have been recorded, including 82 actions during the last six months.

You can access the latest statistics [here](#).

6 Decision of the Brazilian Data Protection Authority Concerning Children’s Personal Data Processed by TikTok/ByteDance

PUBLICATION DATE: 24.08.2026



The Brazilian National Data Protection Authority (“ANPD”) imposed an administrative fine of **BRL 153.7 million** on ByteDance, the parent company of TikTok, for the unlawful processing of personal data relating to children and adolescents. The decision also ordered the deletion of unlawfully collected data and required the company to implement a compliance plan aimed at protecting the personal data of children and adolescents.

The ANPD found that TikTok processed the personal data of children and adolescents without a valid legal basis both in the non-registered user experience and in registered

accounts. It further concluded that the company had failed to demonstrate effective measures to prevent such users from accessing or registering on the platform, as well as sufficient technical and organisational measures to ensure compliance with data protection obligations.



The compliance plan requires, among other measures, stricter privacy settings to be applied by default to accounts of users under the age of 16, stronger parental controls, the suspension of advertising in the non-registered user experience, and restrictions on personal data processing activities.

You can access the full text of the decision [here](#).

7 CNIL Update to Its Traceability Tool for Open-Weight Artificial Intelligence Models

RELEASE DATE: 26.08.2026

The French Data Protection Authority (“**CNIL**”) released an updated version of its Genmod tool, which is designed to trace the origin and derivative relationships of open-weight artificial intelligence models.

The tool aims to identify the models from which an AI model is derived and the models to whose development it has contributed.

! Such traceability is particularly relevant where personal data may have been learned or retained by a model, as the same data may also have been transferred to or retained within derivative models.

The CNIL stated that this approach may contribute to assessing the conditions under which data subjects may exercise their rights under the General Data Protection Regulation (“**GDPR**”).

The updated version improves search performance and the user interface, while model data are now updated automatically on a weekly basis using publicly available information from **Hugging Face**. This is intended to enable more up-to-date and transparent tracking of relationships between models within the open-weight AI ecosystem.

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

8 Transparency and AI Content Labelling Obligations under the EU Artificial Intelligence Act

APPLICATION DATE: 02.08.2026

The transparency obligations set out in Article 50 of the European Union Artificial Intelligence Act (“**AI Act**”) became applicable as of 2 August 2026. The rules aim to ensure that users can clearly understand when they are interacting with AI systems and when certain content has been generated or manipulated by artificial intelligence.

In this context, transparency obligations are particularly relevant to deepfake content, chatbots and AI agents, certain AI-generated text,

as well as emotion recognition and biometric categorisation systems.

The European Commission has also published an icon set and implementation tools for the labelling of AI-generated content, emphasizing that disclosures should be clear, visible and accessible.

You can access further information on the matter [here](#).

CONTACT

EGE ÇAKIRCA ATTORNEYS AT LAW



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



info@eclawtr.com



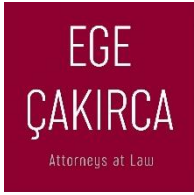
+90 212 352 3318



eclawtr.com



EGE • ÇAKIRCA



Founding Partner
Özlem EGE POLAT



Of Counsel
(Technology and Digital Law)
Hande AKSU



Associate
Ceren AYDEMİR



Legal Trainee
Ezgi OPRUKÇU