Personal Data Protection Bulletin

2026
First Quarter

Sevgi Ünsal Özden
Ozan Akman
Gülnur Çakmak Ergene
Elvan Galatalı
Pelin Mutlu

Current Developments from Türkiye

The Personal Data Protection Authority Published a Public Announcement on the Use of Foreign-Origin Messaging Applications in Public Institutions

In its Public Announcement on the Use of Foreign-Based Communication Applications in Public Institutions, the Personal Data Protection Authority (Authority) shared its assessments regarding recent complaints and notifications received by the Authority. In this context, the complaints received by the Authority indicated that public personnel were being compelled to use WhatsApp for administrative processes, and that orders and instructions were conveyed and official documents were shared through the application.

Referring to Presidential Circular No. 2019/12, the Authority stated that classified data must not be shared through mobile applications and that domestically developed communication applications should be preferred. In this regard, it emphasized that official documents of a classified or critical nature should not be shared via applications such as WhatsApp that do not have data centers located in Türkiye.

The Authority further noted that the sharing of personal data through such applications constitutes a "personal data processing activity" and that activities failing to satisfy the processing conditions under Articles 5 and 6 of the Law on the Protection of Personal Data No. 6698 (KVKK) may be investigated upon complaint or ex officio. The Authority also reminded that public personnel whose responsibility is established may be subject to disciplinary sanctions.

> You can access the announcement published by the Authority in Turkish here.

The Personal Data Protection Authority Published an Announcement Titled "'Quishing': Risks Arising from QR Codes"

The Authority published an announcement on 26 February 2026 warning against phishing attacks conducted through QR codes, commonly referred to as "quishing".

The announcement indicates that individuals may be redirected to malicious websites through fake or subsequently altered QR codes, which may result in the compromise of personal data or the installation of malware on their devices. It is particularly emphasized that dynamic QR codes pose increased risks, as their redirect links can be modified after creation.

The Authority recommends exercising caution with QR codes received from unknown sources, particularly those conveying a sense of urgency, verifying redirected links, maintaining up-to-date device security, and implementing measures such as multi-factor authentication.

> You can access the announcement published by the Authority in Turkish here, and our announcement on this matter here.

Principle Decision on the Use of Loyalty Cards by Third Parties

The Personal Data Protection Board (Board) published its Principle Decision dated 11 February 2026 and numbered 2026/266 regarding the use of loyalty cards by third parties using the card-holder's phone number or membership number during purchases.

The Principle Decision indicates that allowing transactions to be carried out via loyalty cards without the data subject's knowledge or consent and without the implementation of any authentication mechanism does not rely on a valid legal basis under Article 5 of the KVKK. It is further stated that recording purchases not made by the data subject under their account or issuing invoices in their name may give rise to a risk of non-compliance with the principle of accuracy and, where necessary, being up to date. The Board also emphasizes that contractual provisions prohibiting third-party use do not eliminate the data controller's data security obligations under Article 12 of the KVKK.

Accordingly, the Board decided that practices allowing transactions via loyalty cards without verification must be terminated and that appropriate technical and administrative measures should be implemented to verify that the use of loyalty cards is carried out with the data subject's knowledge and consent. A six-month compliance period was granted to data controllers as of the publication of the Principle Decision in the Official Gazette.

You can access the Principle Decision in Turkish here, and our announcement on this matter here.

Key Actions

Data controllers operating loyalty card programs should implement authentication mechanisms such as SMS verification, mobile application authentication, and dynamic barcode/QR code systems during transactions, establish tiered verification processes based on the type of transaction and the level of risk, and revise their membership agreements, privacy notices, and internal policies and procedures in line with the Principle Decision.

The Authority Published an Announcement Titled “Use of Generative AI Tools in the Workplace”

The Authority published a document titled “Use of Generative AI Tools in the Workplace” on 5 March 2026, with the aim of raising awareness regarding the use of generative artificial intelligence tools in workplaces, identifying potential risks, and drawing attention to responsible use approaches, particularly in relation to tools provided by third parties and accessible to the public.

The document emphasizes that while generative AI tools may enhance efficiency in business processes, they may also give rise to various risks in terms of personal data protection, information security, intellectual property, and corporate reputation, particularly in relation to “shadow AI” practices where such tools are used without established corporate policies.

You can access the document in Turkish here, our announcement on this matter here and our Exlibris article on this matter here.

Key Actions

With respect to AI tools used within organizations, it is important to prioritize the use of anonymized data where possible, establish clear and implementable corporate policies, conduct employee training and awareness activities, and ensure the continuation of human oversight over AI-generated outputs.

The Authority Published Guidance on "Agentic AI"

The Authority published a document titled "Agentic AI", addressing the main characteristics of agentic AI systems, the AI agents utilized, their potential areas of use, and the risks they may pose in terms of personal data.

The document indicates that such systems are structures capable of evaluating environmental conditions, planning, and acting with a certain degree of autonomy to achieve specific objectives. These systems are noted to have potential applications in areas such as research and development, customer services, financial analysis, healthcare, and incident response.

However, the Authority emphasizes that the multi-step and goal-oriented nature of such systems may give rise to various risks in terms of predictability, transparency, explainability, data minimization, purpose limitation, and data security.

Accordingly, the importance of human oversight, explainability, data accuracy, clearly defined roles and responsibilities, and the adoption of a privacy-by-design approach is highlighted in the use of agentic AI systems.

> You can access the document in Turkish here and our announcement on this matter here.

The Authority Published Public Announcement on the Registration of Personal Data Processed within Joint Ventures, Consortia, and Ordinary Partnerships in VERBIS

The Authority published a public announcement to eliminate uncertainties arising in practice regarding the notification of personal data processed within the scope of activities carried out under structures such as joint ventures, consortia, and ordinary partnerships to the Data Controllers' Registry Information System (VERBIS).

The announcement indicates that, since such structures do not have separate legal personality, they should not be registered in VERBIS in their own name, and that the registration obligation must instead be assessed separately for each party forming the relevant structure.

> You can access the announcement published by the Authority in Turkish here, and our announcement on this matter here.

Key Actions

With respect to joint ventures, consortia, and ordinary partnerships, it should first be determined whether the parties forming such structures are subject to the VERBIS registration obligation. Where such obligation exists, the relevant parties are required to include personal data processed within the scope of the joint structure's activities in their VERBIS notifications.

Constitutional Court Annulled Provisions on the Processing of Genetic Data under the Criminal Procedure Code

The Constitutional Court, with its decision dated 25 December 2025 and numbered 2025/141 E., 2025/274 K., published in the Official Gazette dated 18 March 2026 and numbered 33200, annulled certain provisions of the Criminal Procedure Code No. 5271 regarding the retention and destruction of genetic examination results, on the grounds that they do not provide sufficient safeguards for the protection of personal data.

The decision indicates that matters such as the retention period of genetic data, procedures for their destruction, the rights of data subjects, and available remedies must be clearly regulated at the statutory level.

The Court further ruled that the annulment decision will enter into force nine months after its publication in the Official Gazette, during which period the relevant legislation is expected to be amended in compliance with the Constitution.

> You can access the decision in Turkish here, and our announcement on this matter here.

The Principle Decision on the Separate Preparation of Explicit Consent and Privacy Notices Published

The Board's Principle Decision dated 18 February 2026 and numbered 2026/347, titled "Principle Decision on the Requirement for Data Controllers to Prepare Explicit Consent and Privacy Notices Separately", was published in the Official Gazette dated 24 March 2026 and numbered 33203.

The decision sets out the principles that data controllers must follow when fulfilling their obligations regarding explicit consent and the obligation to inform. Moreover, it includes examples of good and poor practices in its annex. Finally, it is also stated that, in the event of non-compliance with these principles, administrative action may be taken against the relevant data controllers pursuant to Article 18 of the KVKK.

> You can access the decision in Turkish here, and our announcement on this matter here.

Key Actions

Privacy notices and explicit consent texts should be reviewed and revised in line with the principles set out in the decision. In this context, it is important that privacy notices and explicit consent texts are prepared separately, drafted in a clear and plain language, that explicit consent is not sought where it is not required, and that the relevant texts are tailored to each data controller's specific data processing activities.

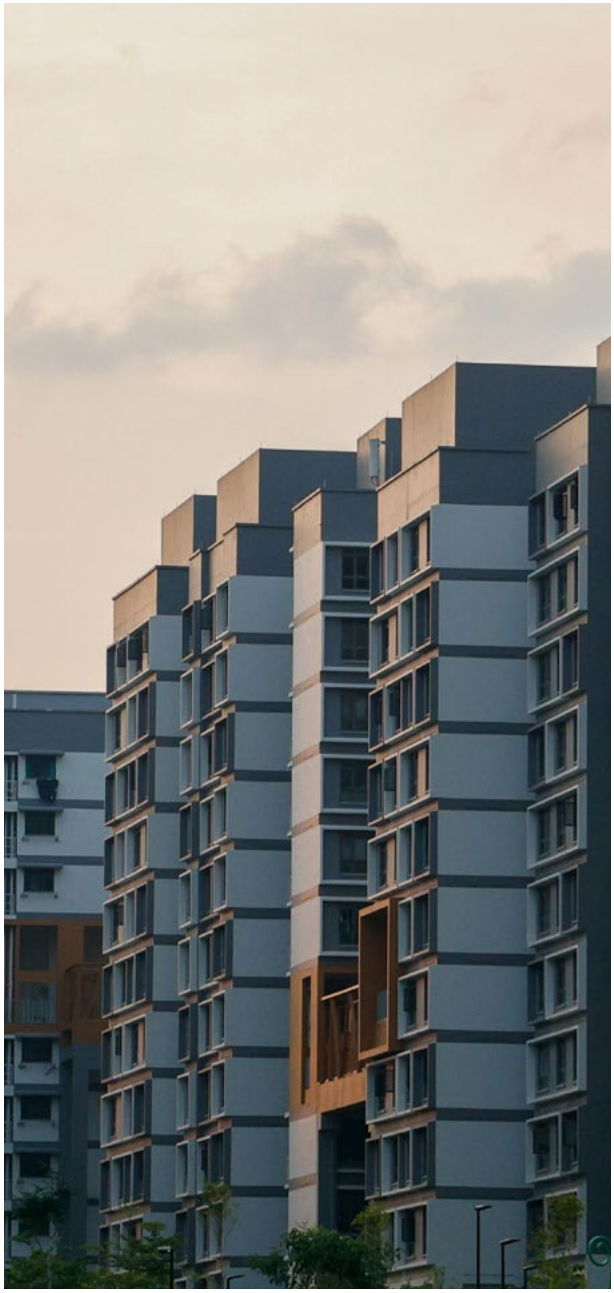
The Principle Decision on the Disclosure of Debt Information Containing Personal Data in Common Areas of Multi-Unit Buildings Published

The Board's Principle Decision dated 18 February 2026 and numbered 2026/348, titled "Principle Decision on the Posting of Debt Information of Apartment/Site Residents in Common Areas in Multi-Unit Buildings," was published in the Official Gazette dated 31 March 2026 and numbered 33210.

The decision assesses, from a personal data protection law perspective, the practice of displaying announcements in common areas regarding dues, advances and similar debts within apartment and residential complex management processes and sets out the principles to be followed in this respect.

Accordingly, the Board emphasizes that informing residents regarding debt information is not entirely prohibited; however, such disclosures must be carried out in compliance with the principle of proportionality and data security obligations. In this context, it is recommended to prefer more secure methods, such as closed e-mail groups, restricted-access messaging groups, or digital systems accessible only to the relevant individuals.

> You can access the decision in Turkish here, and our announcement on this matter here.

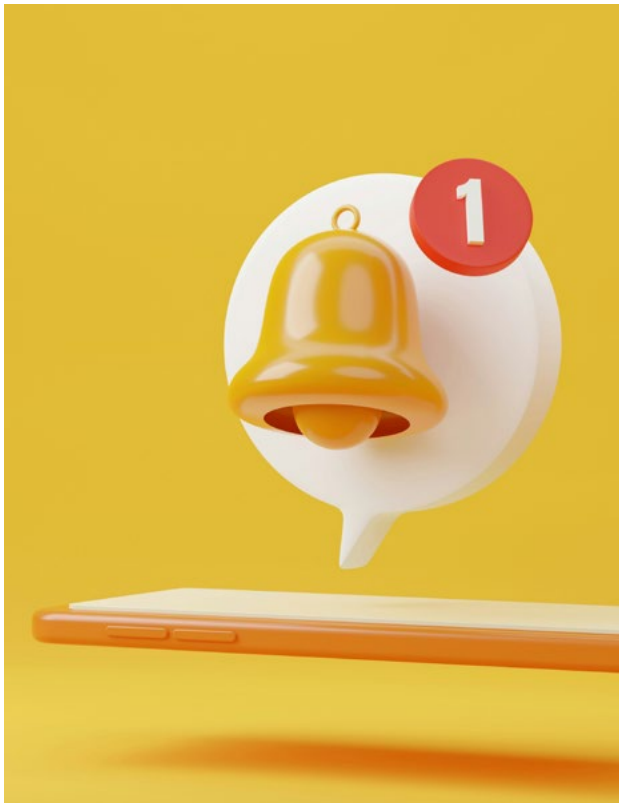


Public Announcement on Push Notifications Sent via Mobile Applications

The Authority published a public announcement on 14 January 2026 following its review of complaints regarding push notifications sent via mobile applications. The announcement emphasizes that mobile application providers, as data controllers, must ensure that their data processing activities comply with the general principles and legal bases set out under KVKK. In this context, push notifications rely on user consent and involve the processing of personal data.

Furthermore, in its announcement, the Authority referred to a specific case it examined and noted that multiple purposes were presented under a single consent and that there were practices whereby users were required to accept marketing communications to access the service. The Authority noted that such practices may undermine the "freely given" nature of consent.

In this context, attention was drawn to the principle of "granular consent," emphasizing that separate consent should be obtained for each data processing purpose and that users should be provided with options to manage their notification preferences. Accordingly, data controllers are therefore encouraged to review their consent mechanisms and separate notification purposes.



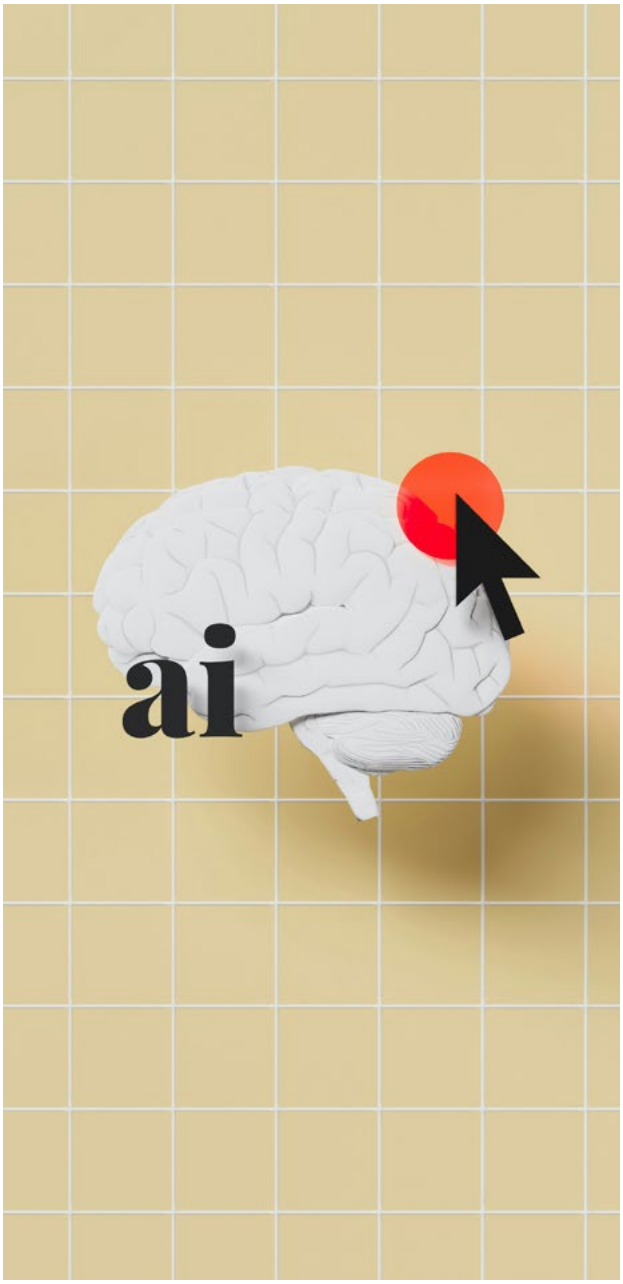
You can access the announcement published by the Authority in Turkish here, and our announcement on this matter here.

Current Developments in the World

Council of Europe Published Handbook on Human Rights and Artificial Intelligence

The Council of Europe has published its Handbook on Human Rights and Artificial Intelligence, developed by the Steering Committee for Human Rights (CDDH) as a practical reference tool for Council of Europe member States. The Handbook is structured around the key rights and freedoms enshrined in the European Convention on Human Rights (ECHR) and the European Social Charter and systematically examines how each right may be affected by the design, development, and deployment of AI systems. It addresses, among others, the right to a fair trial, freedom of expression, the right to privacy, the prohibition of discrimination, and social and economic rights, providing concrete examples of AI-related risks in each area.

The Handbook also considers the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law (CETS No. 225) and includes practical tools such as checklists and guiding questions designed to assist policymakers and public authorities in conducting human rights impact assessments of AI systems. Sector-specific guidance is provided across areas including justice, law enforcement, healthcare, education, and employment, with particular emphasis on the obligations of States to ensure transparency, meaningful human oversight, accountability, and access to effective remedies, regardless of whether AI systems are operated by public or private actors.



You can access the Handbook here.

OECD Published Due Diligence Guidance for Responsible AI

The Organization for Economic Co-operation and Development (OECD) has published its 2026 Due Diligence Guidance for Responsible AI, which provides a practical framework for multinational companies to manage AI-related risks in line with responsible business conduct (RBC) principles. Building on the OECD MNE Guidelines, the guidance adopts a flexible, risk-agnostic approach that can be applied across sectors and AI systems, helping organizations identify, assess, and address potential adverse impacts throughout the AI lifecycle.

The guidance outlines a continuous six-step due diligence process: embedding policies, identifying risks, mitigating impacts, monitoring outcomes, communicating actions, and ensuring remediation, and aims to support innovation, align existing governance frameworks, and offer a common reference point for AI risk management across jurisdictions.

> You can access the guidance published by OECD here.

EU-UK Signed Memorandum of Understanding on Cross-Border Oversight of Critical ICT Providers

In January 2026, EU and UK financial regulators entered a Memorandum of Understanding (MoU) to strengthen cross-border supervision of critical ICT third-party providers (CTPPs) under the Digital Operational Resilience Act (DORA) and the UK critical third-party (CTP) regime. The MoU primarily targets technology providers of critical importance to the operational continuity of the financial sector, including, in particular, companies providing cloud computing services, data storage and data center infrastructure, payment system infrastructure, cybersecurity solutions, and financial software services. The MoU establishes a framework for enhanced cooperation, including systematic information sharing, coordinated inspections, and joint oversight activities, aiming to reduce supervisory gaps and improve operational resilience. It also clarifies that information exchange will remain confidential but may be shared where legally required. For CTPPs such as Amazon Web Services, Microsoft Azure, and Google Cloud, this means closer regulatory scrutiny, more integrated supervision across jurisdictions, and a need to ensure consistency in compliance approaches, documentation, and internal coordination between EU and UK regulatory engagements.

> You can access the announcement here.

Reforms to UK Data Protection and Privacy Laws Come into Force

In February 2026, the UK introduced significant data protection reforms through the Data (Use and Access) Act 2025 (DUAA), marking a divergence from the EU regime. The changes bring greater flexibility in areas such as cookie use, automated decision-making (ADM), and research-related data processing, while strengthening compliance requirements particularly regarding children's data and enhanced enforcement powers of the Information Commissioner's Office (ICO).

Key updates include new cookie consent exceptions, statutory recognition of "stop the clock" for data subject access requests (DSARs), expanded use of ADM with safeguards, clearer research definitions (including commercial research), and a defined list of legitimate interests that reduce the need for balancing tests. Overall, the reforms aim to modernize the framework, offering both compliance relief and increased regulatory scrutiny, with further guidance from the ICO expected.

You can access the DUAA here.

Court of Justice of the European Union Confirms Judicial Review of EDPB Binding Decisions

On 10 February 2026, the Court of Justice of the European Union (CJEU) delivered a landmark judgment confirming that companies may challenge binding decisions of the European Data Protection Board (EDPB) before EU courts, in particular the General Court, under Article 263(1) TFEU, even prior to the adoption of a final decision by their lead supervisory authority.

The case arose from an investigation by the Irish Data Protection Commission into WhatsApp's compliance with its transparency obligations, following which the EDPB adopted a binding decision identifying multiple infringements of the General Data Protection Regulation (GDPR) and requiring the imposition of a EUR 225 million fine. The CJEU found that the decision in question produces directly binding legal effects on the companies concerned without leaving any discretion to national supervisory authorities and held that EDPB decisions of this nature constitute reviewable acts that may be challenged directly before the EU courts. This judgment confirms the availability of substantive judicial review of EU-level GDPR enforcement and is expected to lead to dual-track litigation, with parallel proceedings before EU courts challenging EDPB decisions and before national courts reviewing national implementing decisions.

You can access the CJEU judgment here.

European Commission Updates Draft Code of Practice on AI-Generated Content

On 3 March 2026, the European Commission published the second draft of the Code of Practice on the marking and labelling of AI-generated content, developed to support compliance with the transparency obligations under Article 50 of the AI Act. Compared to the first version, the updated draft adopts a more flexible and practical approach, aiming to simplify compliance processes for providers and deployers of AI systems. The draft provides guidance on the marking and labelling of AI-generated or manipulated content, including requirements to clearly label deepfakes and certain types of AI-generated content. Following a public consultation period that ended on 30 March 2026, the final version is expected to be published in June 2026. The relevant transparency obligations under the AI Act are scheduled to become applicable on 2 August 2026.

> You can access the draft published by the European Commission here.

European Commission Publishes Draft Guidance on the Cyber Resilience Act

On 3 March 2026, the European Commission published draft guidance aimed at clarifying the application of the Cyber Resilience Act (CRA) and supporting stakeholders in understanding their compliance obligations. The draft guidance provides further clarification on the scope of the CRA, confirming its applicability to products with digital elements, including both hardware and software. It also elaborates on key compliance requirements such as risk assessments, vulnerability management, incident reporting obligations, and cybersecurity measures throughout the product lifecycle. In addition, the guidance addresses practical issues such as open-source software, remote data processing solutions, and support periods, while aiming to facilitate compliance, particularly for small and medium-sized enterprises.

The draft was subject to public consultation, with the feedback period closing on 31 March 2026. It is expected to play a key role in shaping the implementation of the CRA. Certain obligations, such as vulnerability and incident reporting, are scheduled to take effect from 11 September 2026. The guidance, even once finalized, will remain non-binding.

> You can access the draft guidance here.

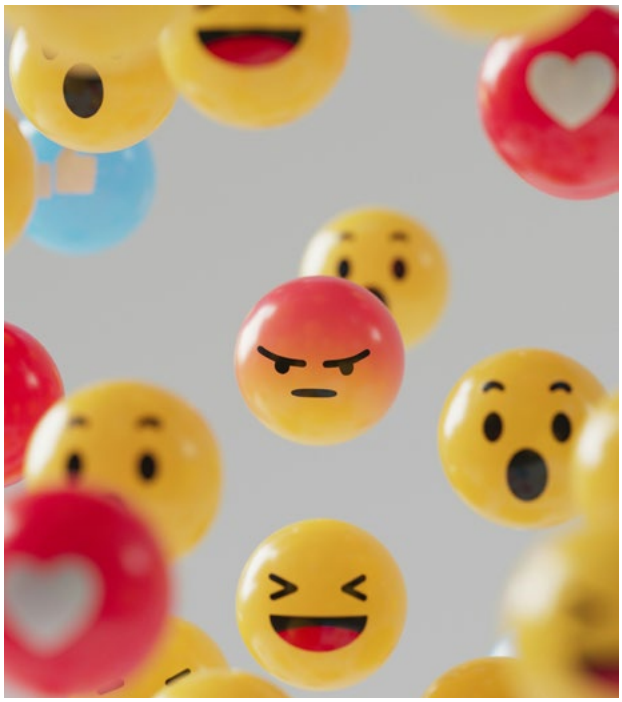
CJEU Clarifies When Data Subject Access Requests May Be Considered "Excessive" under the GDPR

On 19 March 2026, the CJEU clarified when DSARs may be considered "manifestly unfounded or excessive" under the GDPR. The Court confirmed that the number of requests alone is not sufficient to classify them as excessive. Instead, the key factor is whether the request constitutes an abuse of rights. In this context, even a first request may be deemed excessive where it is made for purposes unrelated to data protection, such as pursuing a damages claim. The judgment also emphasizes that refusing a request or charging a fee remains exceptional, with the burden of proof resting on the controller. Publicly available information may be considered but cannot, on its own, justify refusal.

> You can access the CJEU judgment here.

ICO Issues Guidance on the Use of Automated Decision-Making in Recruitment

On 6 February 2026, the European Commission preliminarily found that TikTok may be in breach of the Digital Services Act (DSA) due to features that may contribute to addictive user behavior. The assessment focuses on elements such as infinite scroll, autoplay, push notifications, and personalized recommender systems. The Commission considers that TikTok did not adequately assess the risks these features pose, particularly for minors, nor implement effective mitigation measures. Structural changes, including limiting certain features and improving user controls, may be required. These findings are preliminary, and TikTok has the right to respond. If confirmed, the Commission may impose fines of up to 6% of global annual turnover.



> You can access the guidance published by the ICO here.

ICO Issues Guidance on the Use of Automated Decision-Making in Recruitment

On 31 March 2026, the ICO published guidance addressing the use of ADM and AI in recruitment processes. The ICO notes that employers are increasingly using automated tools to screen CVs, assess candidates, and filter applications. While such tools may improve efficiency, they also raise concerns regarding transparency, fairness, and the risk of bias or discrimination. According to the ICO, the use of ADM in recruitment may be permissible provided that appropriate safeguards are in place. These include clearly informing candidates about the use of automated tools, ensuring transparency in decision-making processes, and enabling individuals to challenge decisions and request human review. The ICO also encourages organizations to review their recruitment practices and ensure compliance with data protection requirements when deploying such technologies.

You can access the guidance published by the ICO here.

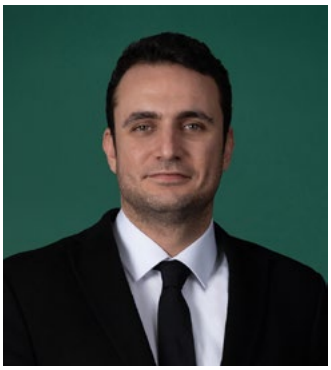
Key Actions

With respect to organizations utilizing ADM and AI tools in recruitment processes, it is important to identify the stages at which automated tools are deployed such as CV screening, scoring, and shortlisting and to clearly inform candidates of these processes; to provide candidates who are eliminated through automated assessments with the opportunity to learn the reasoning behind the decision and to request a reassessment by a human reviewer; to regularly test whether the algorithms used produce discriminatory outcomes with respect to protected characteristics such as age, gender, disability, and ethnicity; to document and periodically review automated screening thresholds and scoring criteria; and to conduct data protection impact assessments in relation to existing recruitment processes and implement the necessary technical and administrative measures.

Key Contacts

Sevgi Ünsal Özden
Managing Associate and Mediator

sevgiunsal@erdem-erdem.com



Ozan Akman
Senior Associate

ozanakman@erdem-erdem.av.tr

Disclaimer

ERDEM & ERDEM

40 YEARS

İSTANBUL

Ferko Signature
Büyükdere Caddesi, No. 175 Kat. 3
34394, Esentepe - Şişli, İstanbul

+90 212 291 73 83
+90 212 291 73 82

istanbul@erdem-erdem.av.tr

İZMİR

1476 Sokak, No. 2, D. 27, Aksoy
Plaza Alsancak, İzmir

+90 232 464 66 76
+90 232 466 01 21

izmir@erdem-erdem.com

AMSTERDAM

Office 4.31, Strawinskylaan 457,
1077 XX Amsterdam

+31 (0)20 747 1113

amsterdam@erdem-erdem.nl

www.erdem-erdem.av.tr