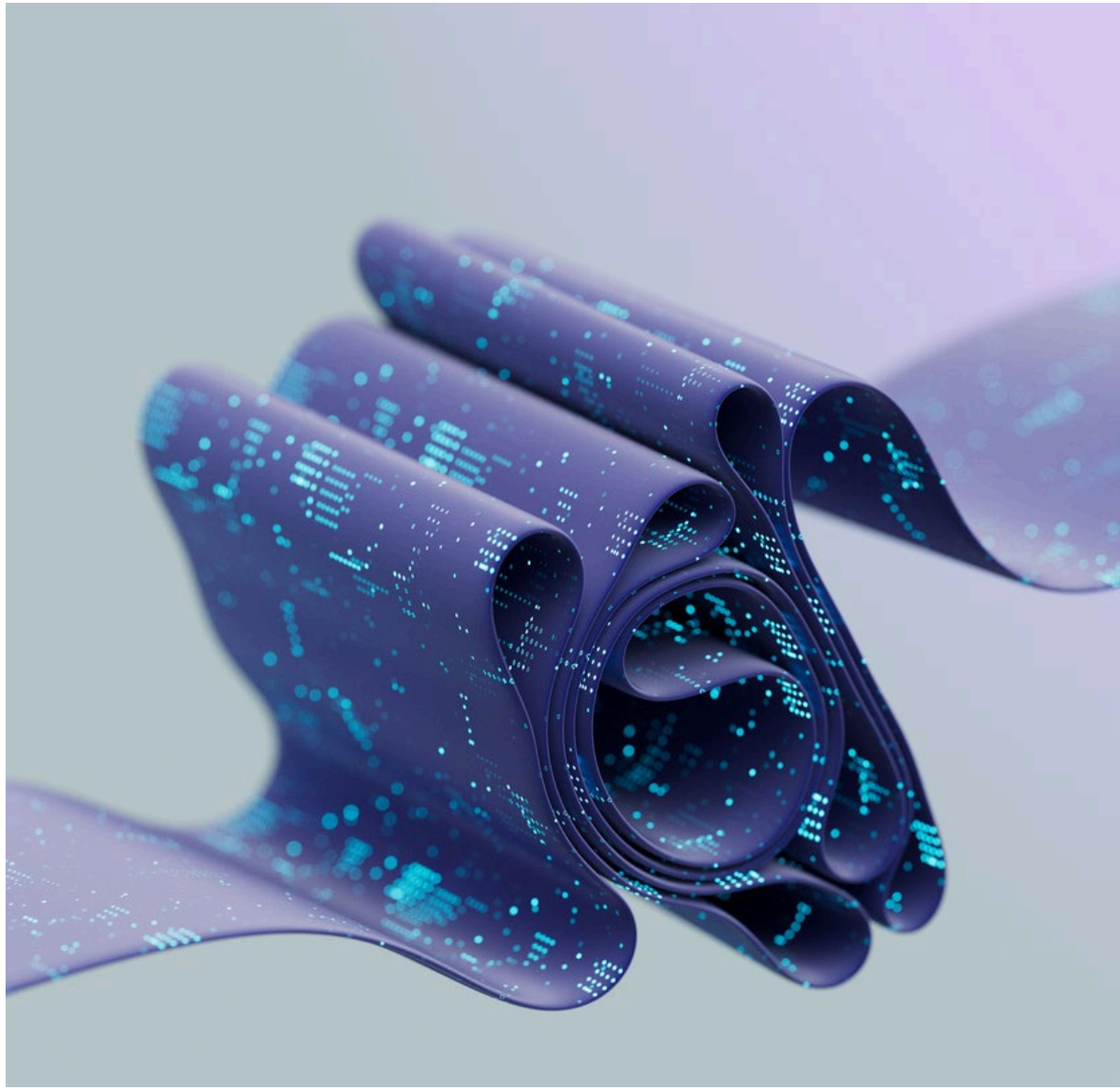
MARIF

Tech & Data Law Quarterly

Q1 | 2026

MARIF

Contents



Constitutional Court Decisions - Publication of Exam Results and Freedom of Expression

Date: 16 February 2026

Summary

The Constitutional Court examined whether the administrative fine imposed in relation to the publication of a student's personal data in a news article violated freedom of expression and freedom of the press, and concluded that no violation had occurred. The Decision highlights the need to balance freedom of expression with the protection of personal data and emphasises the importance of necessity and proportionality in such assessments.

Details

The Constitutional Court examined an individual application alleging that the administrative fine imposed by the Personal Data Protection Board, following the publication of an exam results document belonging to an individual in a news article on an online news website, violated freedom of expression and freedom of the press. Following its review, the Constitutional Court concluded that there had been no violation of those freedoms.

The Decision emphasised that a balance must be struck between freedom of expression and the right to the protection of personal data. It was assessed that, although the news concerned a student's success, it did not contribute to a matter of public debate. On the other hand, the Court found that personal data belonging to the individual concerned, such as their full name, photograph, university and programme information, and placement score, had been clearly disclosed, and that no justification had been provided as to why this disclosure was necessary.

Within this framework, the Court concluded that the administrative fine imposed pursued a legitimate aim, was compatible with the requirements of a democratic society and was proportionate. Accordingly, it held that freedom of expression, considered in the light of freedom of the press, had not been violated.

You may access the full text of the decision here.

MARIF

Constitutional Court Decisions - Annulment of Provisions on Genetic Data Retention

Date: 18 March 2026

Summary

The Constitutional Court annulled provisions regulating the retention and destruction of genetic data on the grounds that they lacked sufficient safeguards for the protection of special categories of personal data. The Decision emphasises the need for a clear legal framework governing the processing and protection of such data.

Details

The Constitutional Court examined Article 80(2) and Article 82 of the Code of Criminal Procedure, which regulate the retention and destruction of data obtained through molecular genetic examinations, and annulled these provisions on the grounds that they do not provide sufficient safeguards for the protection of personal data.

The provisions in question stipulated that data obtained as a result of molecular genetic examinations conducted for the purpose of obtaining evidence in relation to a criminal offence must be destroyed immediately upon the expiry of the objection period against a decision of non-prosecution, the rejection of such objection, or the issuance and finalisation of a decision of acquittal or a decision that there is no need to impose a penalty.

In its Decision, the Court emphasised that data obtained through molecular genetic examinations constitute special categories of personal data and therefore require stricter safeguards. While the provisions required the destruction of such data upon the finalisation of certain decisions, the Court found that the law does not establish a clear framework regarding how such data should be retained, under which conditions they may be processed, or how the rights of data subjects are to be safeguarded.

The Court further stated that, since personal data processed by judicial authorities or enforcement bodies in the context of investigation, prosecution, trial or execution proceedings fall within the exceptions regulated under Law No. 6698, the necessary safeguards for such data must be clearly regulated by law.

Accordingly, the provisions in question were found to be in breach of Articles 13 and 20 of the Constitution and were annulled. The Court also ruled that the annulment will enter into force nine months after the publication of the Decision in the Official Gazette, which took place on 18 March 2026.

You may access the full decision here.

MARIF

Personal Data Protection Board Decisions - Loyalty Card Programs and Identity Verification Requirements

Date: 11 February 2026

Summary

The Personal Data Protection Board ("**Board**") evaluated practices within loyalty card programmes and identified risks arising from transactions carried out by using only phone numbers or loyalty card numbers, without adequate verification.

Details

Through its Principle Decision dated 11 February 2026 and numbered 2026/266, the Board evaluated certain practices within loyalty card programmes. According to the Decision, in some cases purchases made through such programmes can be completed merely by providing the data subject's mobile phone number or loyalty card number at the checkout, which may enable third parties to carry out transactions without the knowledge or consent of the data subject. The Decision further notes that, as a result of such transactions, invoices or similar documents may be issued in the name of the loyalty card holder and customer transaction data relating to the purchase may be recorded in the data subject's records or membership account.

The Board considered that such practices may lead to unlawful personal data processing activities and personal data breaches and stated that data controllers should implement identity verification mechanisms for the use of loyalty cards, such as SMS verification codes or the scanning of a barcode/QR code through a mobile application or website. The Board also granted data controllers a six-month compliance period, starting from the publication of the Principle Decision, to establish the necessary verification mechanisms.

You may access the full text of the Principle Decision here.

Conclusion

Data controllers should review their loyalty card infrastructures and use the compliance period granted by the Board to implement secure identity verification mechanisms that prevent unauthorised use and mitigate the risk of unlawful data processing and potential data breaches.

Personal Data Protection Board Decisions - Explicit Consent and Privacy Notices

Date: 18 February 2026

Summary

The Board emphasised that explicit consent texts and privacy notices must be prepared separately due to their distinct legal nature and function. The Decision underlines that combining these texts into a single combined approval mechanism is a common but non-compliant practice and clarifies how such documents should be structured and presented.

Details

Through its Principle Decision dated 18 February 2026 and numbered 2026/347, titled “Principle Decision on the Requirement for Data Controllers to Prepare Explicit Consent Texts and Privacy Notices Separately,” the Board provided important guidance on common errors frequently encountered in practice. The Principle Decision emphasises that explicit consent texts and privacy notices differ in their legal nature: while the disclosure obligation is an obligation to inform individuals whose personal data are processed, explicit consent is only one of the legal grounds for personal data processing.

In this context, the Board clearly stated that presenting these two texts as a single combined approval text may be considered contrary to the Law. It further indicated that the disclosure obligation must be fulfilled separately, prior to the commencement of the data processing activity, regardless of the legal basis relied upon. Explicit consent, by contrast, should only be obtained where necessary and as a separate declaration of intent. Accordingly, the Board stated that privacy notices and explicit consent texts must be prepared under separate headings and as distinct declarations.

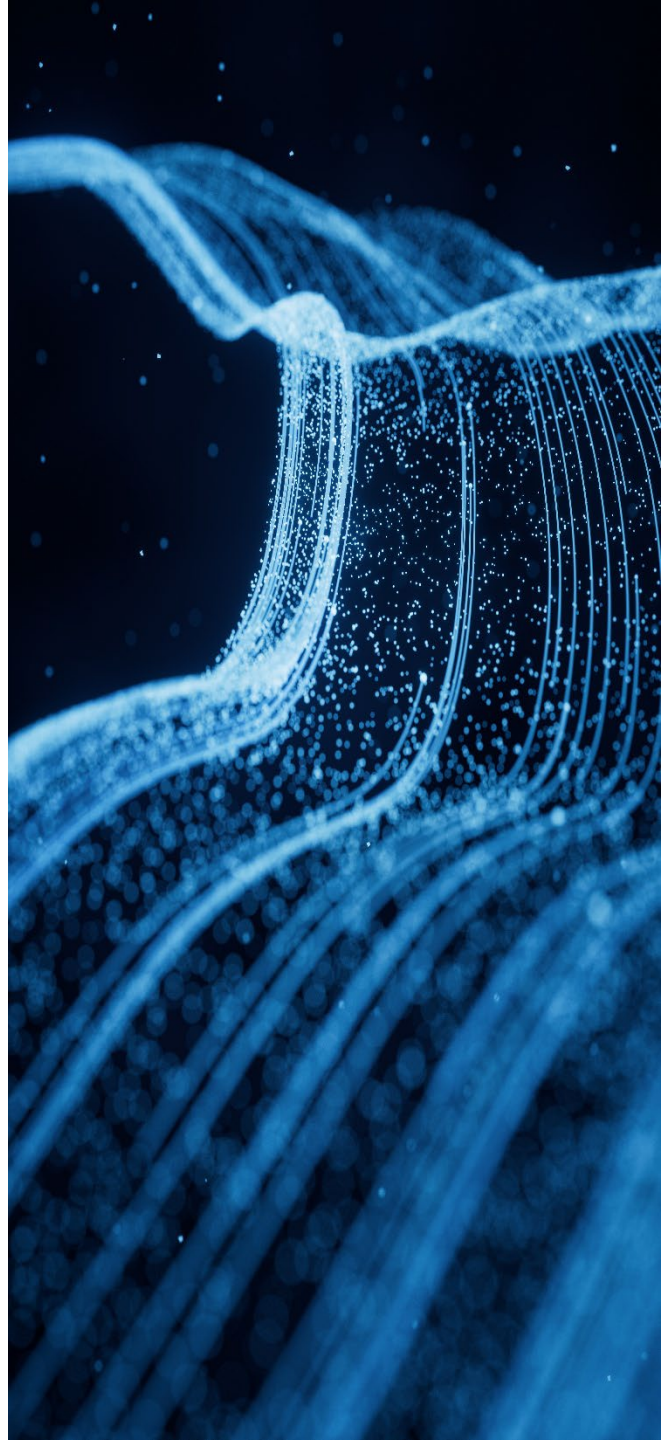
The Board further noted that, although it is possible to present the privacy notice and the explicit consent text on the same page, this is subject to the condition that the two texts are clearly distinguished from each other and structured as separate declarations of intent. In this regard, the Board stated that data controllers may only obtain confirmation that data subjects have read and understood the privacy notice; however, the use of statements such as “I have read and accept”, or similar expressions that may associate the privacy notice with explicit consent, may be considered contrary to the Law.

The Principle Decision also includes examples of good and bad practices in order to guide data controllers and sets out, through concrete templates, how such texts should be prepared. The Board further indicated that it may initiate action against data controllers if practices contrary to the principles set out in the Principle Decision are identified.

You may access the full text of the Principle Decision here.

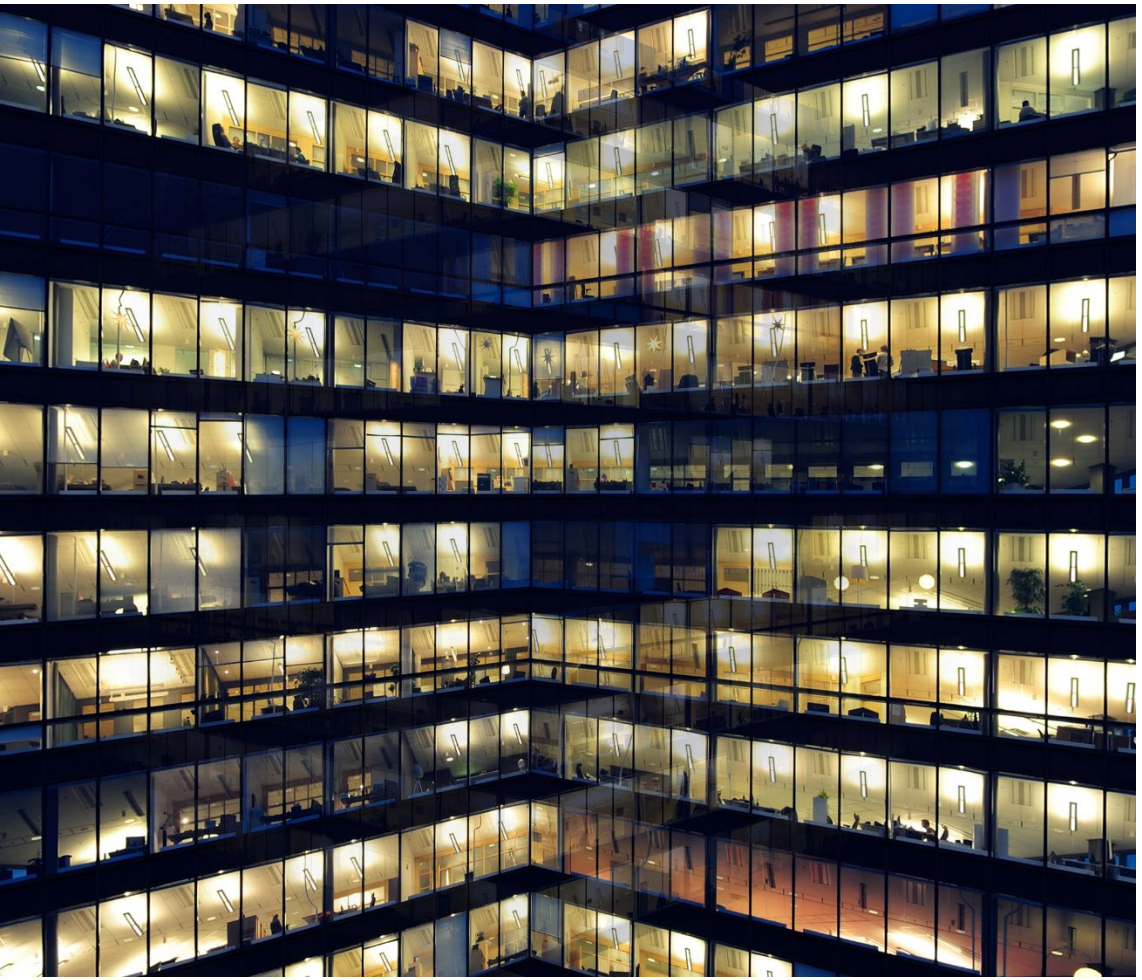
Conclusion

Data controllers should reassess their data collection interfaces and documentation, including online forms, checkbox flows and layered notice structures, to ensure that privacy notices and explicit consent mechanisms are clearly separated and compliant with the Board’s guidance.



Personal Data Protection Board Decisions - Display of Debt Information in Common Areas

Date: 18 February 2026



Summary

The Board evaluated the display of residents' debt information in common areas and concluded that such practices may result in the unlawful disclosure of personal data to third parties. The Decision highlights that publicly accessible areas within residential complexes should not be used for sharing personal information.

Details

Through its Principle Decision dated 18 February 2026 and numbered 2026/348 on the Display of Debt Information of Apartment/Site Residents in Common Areas in Collective Living Spaces, the Board evaluated the practice of apartment and residential complex managements displaying dues, advances and similar debt information in common areas from a personal data protection law perspective.

In the Decision, the Board assessed Law No. 6698 together with the Condominium Law and stated that, while a certain level of notification is necessary for tracking common expenses and protecting the rights of condominium owners, the display of personal data such as name and surname, apartment number, debt amount and delay period in areas accessible to everyone, such as elevators, building entrances or corridors, is not compliant with the Law.

The Board emphasised that such practices make personal data accessible not only to condominium owners but also to guests, couriers and other third parties, and that this may result in a breach of the applicable data processing conditions and data security obligations.

In this context, the Board stated that such practices must cease without delay, that existing lists must be removed from common areas, and that notifications should be made only through closed communication channels accessible to the relevant persons, such as email, messaging groups or applications specifically designed for this purpose. The Board also stated that administrative action may be taken against data controllers acting in breach of these obligations pursuant to Article 18 of the Law.

You may access the full text of the Principle Decision here.

Conclusion

Apartment and residential complex managements should immediately cease public disclosure practices and adopt restricted-access communication methods to ensure compliance with personal data protection requirements.

MARIF

Announcements from the Data Protection Authority - Push Notification and Consent Requirements

Date: 14 January 2026

Summary

The Personal Data Protection Authority ("**Authority**") emphasised that separate and specific consent must be obtained for different types of push notifications, in particular by distinguishing operational notifications from marketing notifications. The announcement highlights that bundled consent mechanisms are not valid.

Details

The Authority published a public announcement on 14 January 2026 regarding push notifications sent to users via mobile applications. The announcement emphasises that notifications sent through mobile applications are based on permissions granted by users through their devices and that the personal data processing activities carried out within this scope must comply with the Law.

The Authority further stated that, in a case under examination, operational notifications and promotional notifications were presented under a single consent mechanism, which resulted in users being required to accept marketing notifications in order to receive operational notifications. It stated that, for consent to be valid, data controllers must present consent mechanisms for push notifications separately for each purpose in a clear and understandable manner, provide users with the ability to customise and select which types of notifications they wish to receive through in-app settings or device operating system settings, and structure their applications accordingly.

You may access the public announcement here.

Announcements from the Data Protection Authority - Investigation into Google Assistant

Date: 11 February 2026

Summary

The Authority announced that it has launched an *ex officio* investigation into Google LLC concerning Google Assistant. The investigation focuses on allegations that unintended activations of the voice assistant may lead to the recording of users' private conversations without consent and the subsequent use of such data for purposes including targeted advertising.

Details

The Authority, in its public announcement published on 11 February 2026, stated that an *ex officio* investigation has been initiated against Google LLC in relation to allegations reflected in the public concerning Google Assistant, Google's voice assistant.

It was noted that, although Google Assistant is intended to be activated by trigger phrases such as "Hey Google / Ok Google", certain reports indicate that false activations may result in users' private conversations being recorded without their consent and that such recordings may be used for targeted advertising and other purposes.

In this context, the Board stated that it had initiated an ex officio investigation against Google LLC in order to assess whether the technical and administrative measures required under the Law have been implemented and whether the relevant personal data processing activities comply with the Law.

You may access the public announcement here.

Announcements from the Data Protection Authority - Investigation into Grok AI

Date: 11 February 2026

Summary

The Authority announced that an *ex officio* investigation has been initiated in relation to the Grok AI platform, focusing on allegations concerning the generation of non-consensual explicit content and the potential unlawful processing of personal data.

Details

The Authority, in its public announcement dated 11 February 2026, stated that an investigation has been initiated in relation to the Grok Artificial Intelligence Assistant, an artificial intelligence platform developed by X.AI Corporation.

The announcement states that the Grok platform has reportedly been subject to an investigation initiated by the European Commission on the grounds that it may have been used to generate sexually explicit images and videos without the consent of individuals, including children, and that such content may have been circulated.

In this context, the Board stated that it had decided to initiate an ex officio investigation into X Internet Unlimited Company and X.AI Corporation in order to assess whether the technical and administrative measures required under Personal Data Protection Law No. 6698 ("**Law**") were taken during the development and use of Grok, and whether the relevant personal data processing activities comply with the Law.

You may access the public announcement here.

Use of Generative AI Tools in the Workplace

Date: 5 March 2026

Summary

The Authority published guidance document on the use of generative artificial intelligence tools in the workplace. The document outlines the increasing role of such tools in business processes, highlights the risks arising from uncontrolled use and provides recommendations for organisations to ensure responsible and secure use.

Details

The Authority's guidance addresses the increasing use of generative AI tools in workplace practices and highlights that such tools, which can generate text, images, audio and code, are widely used to support tasks such as drafting content, summarising documents and assisting with research. While these tools provide efficiency gains, their use may also create risks that require careful management.

A key focus of the document is the concept of "shadow AI", referring to the use of generative AI tools by employees without organisational knowledge or oversight. The Authority notes that this type of use may limit visibility and control over how such tools are used, what data is shared and how outputs are incorporated into business processes.

The guidance identifies several risk areas, including the potential disclosure of personal data and confidential business information, reduced reliability of outputs and challenges in ensuring accountability. It is also emphasised that AI-generated outputs may be inaccurate or misleading and should not be relied upon without appropriate human review.

In this context, the Authority recommends that organisations adopt structured and balanced approaches rather than prohibiting the use of such tools altogether. Suggested measures include establishing clear internal policies, defining permissible use cases, limiting the sharing of sensitive data, implementing access controls and promoting employee awareness through training and guidance.

You may access the guidance document here.

Conclusion

Organisations should assess the use of generative AI tools within their operations and establish clear internal frameworks governing their use. In particular, adopting defined policies, ensuring employee awareness and maintaining control over data shared with such tools will be essential to mitigating risks. A balanced and well-structured approach will enable organisations to benefit from these technologies while maintaining compliance and safeguarding information security.

Amendments to the Presidential Decree on the Cyber Security Presidency

Date: 25 December 2025

Summary

Following the establishment of the Cyber Security Presidency under Presidential Decree No. 177 and the enactment of the Cyber Security Law No. 7545, a further amendment was introduced through Presidential Decree No. 192. The amendment expands the duties and powers of the Cyber Security Presidency, particularly in relation to digital governance and public sector transformation.

Details

Presidential Decree No. 192, published in the Official Gazette dated 25 December 2025, introduces amendments to the existing legal framework governing the Cyber Security Presidency. The changes broaden the scope of the Presidency's responsibilities beyond traditional cybersecurity functions.

Under the amended framework, the Presidency is entrusted with duties relating to digital state architecture, including the establishment of institutional standards for public IT systems, the development of national policies and strategies and ensuring coordination among relevant institutions. The Presidency is also authorised to contribute to the alignment of domestic regulations with international standards and to coordinate relevant institutions.

The amendments further introduce responsibilities in areas such as artificial intelligence and data governance. In this context, the Presidency is expected to play a role in shaping regulatory frameworks, setting data standards and contributing to the development of national strategies concerning emerging technologies.

In addition, responsibilities relating to the development and operation of e-Government (e-Devlet) system and shared digital public services and infrastructures have been included within the scope of the Presidency's mandate.

Additionally, the organisational structure of the Presidency has been updated, including provisions allowing the establishment of domestic and international units and the creation of new departments such as those focusing on artificial intelligence and digital state functions.

You may access the amendment here.

Conclusion

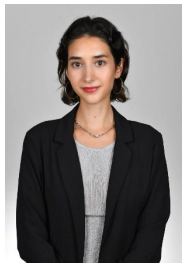
The amendments significantly expand the role of the Cyber Security Presidency, positioning it as a central authority not only in cybersecurity but also in the broader digital transformation of the public sector. The Presidency is expected to take on an increasingly active role in shaping policy, setting standards and coordinating institutional efforts in the coming period.

MARIF

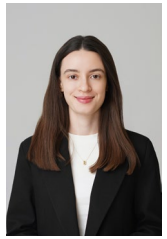
CONTACTS

A. Oktay Uğurlu
Founding Partner
+90 212 280 2434
ougurlu@mariflaw.com

Gökhan Akçaalan
Partner
+90 212 280 2434
gakcaalan@mariflaw.com



Nehir Atalay
Associate
+90 212 280 2434
natalay@mariflaw.com



Begüm Güngör
Associate
+90 212 280 2434
bgungor@mariflaw.com

Sueda Yener
Associate
+90 212 280 2434
syener@mariflaw.com

MARIF

MARIF Law Firm
Büyükdere Caddesi
No: 127 Astoria A Kule 2101
Kat: 21 Esentepe 34394 Şişli
Istanbul, Turkey

+90 212 280 2434
mariflaw.com