AMENDMENTS TO THE PERSONAL DATA PROTECTION LAW

The long-awaited and significant amendments to the Turkish Personal Data Protection Law ("**PDPL**") were published on 12 March 2024, through the Amendment Law on the Code of Criminal Procedure and Certain Laws ("**Amendment Law**"). In general, the new regulations introduced by the Amendment Law will come into effect on 1 June 2024.

The Ministry of Treasury and Finance, along with the Presidency of Strategy and Budget, periodically prepare the Medium - Term Program, which includes the economic and social policies, principles, and goals that private sector and public sector in Turkey should follow to strengthen Turkey's economic stability. The Medium - Term Program of 2024-2026 foresees the completion of PDPL's compliance with the General Data Protection Regulation ("**GDPR**") by the end of the 4th quarter of 2024. The Medium-Term Program also aims to address urgent issues before the end of the 4th quarter of 2024. Hence, compliance with GDPR's cross-border data transfer rules has been prioritized with the Amendment Law. Upon reviewing the objectives outlined in the 2024-2026 Medium-Term Program, it becomes evident that the Amendment Law has addressed urgent concerns related to the processing of personal data. Additionally, a more comprehensive amendment is expected in the future to ensure full compliance of the GDPR.

The Amendment Law changes the rules regarding cross-border data transfers, the processing of sensitive personal data, and the appeal process against the decisions of the Personal Data Protection Board ("**Board**") and these changes are summarized below.

1. New Legal Grounds for Processing Sensitive Personal Data

In principle, according to the PDPL, sensitive personal data such as health and sexual life data, biometric and genetic data, membership to associations, foundations or trade-unions, criminal data can only be processed with the explicit consent of the data subjects. PDPL also regulates legal grounds to process sensitive personal data without explicit consent. Accordingly, (i) sensitive data, except health and sexual life data, can be processed by data controllers without explicit consent only if it was explicitly regulated by laws, and (ii) health and sexual life data can be processed without the explicit consent only by the individuals subject to confidentiality obligations or competent public institutions and organizations for the purposes of the protection of public health, the operation of preventive medicine, the medical diagnosis, treatment and nursing services and the planning, financing and management of health-care services.

The Amendment Law introduced new legal grounds for processing sensitive personal data to ensure compliance with GDPR. Additionally, the conditions for processing health and sexual life data were standardized with those for other sensitive personal data. The newly introduced legal ground of "necessity of processing personal data to fulfil legal obligations in the field of employment, occupational health and safety, social security, social services, and social assistance" aims to alleviate operational challenges faced by data controllers who are employers. With this amendment, employers are no longer obliged to obtain explicit consent from employees for processing sensitive personal data through HR department personnel during the recruitment process, particularly for fulfilling occupational health and safety requirements.

Following the enactment of the Amendment Law, sensitive personal data may be processed under various legal grounds, including explicit consent from data subjects, explicit provisions in laws, and the necessity to process sensitive personal data for the establishment, exercise, or protection of a right.

2. Cross-Border Data Transfer

In accordance with the PDPL, as a rule, personal data cannot be transferred abroad without the explicit consent of the data subjects. PDPL also regulates legal grounds to transfer personal data abroad without explicit consent. Accordingly, (i) personal data can be transferred to a third party with an adequate level of protection according to the safe country list to be published by the Board if the legal grounds regulated under Articles 5 or 6 of the PDPL exists or (ii) personal data can be transferred to a third party without an adequate level of protection according to the safe country list to be published by the Board by executing cross-border data transfer commitment between the parties involved and submitting it to the Board for approval.

The fact that the safe country list, which determines countries with an adequate level of protection has not yet been announced, along with the lengthy approval process of the commitments and obtaining explicit consent from the data subjects, poses several operational challenges for the data controllers, especially those providing cloud services and software from third parties residing

abroad. The Amendment Law aims to align the cross-border data transfer rules of the PDPL with GDPR to eliminate these operational challenges. Under the Amendment Law, personal data can be transferred to third parties without obtaining explicit consent if one of the following conditions is met:

(i) Presence of the Board's adequacy decision regarding the country, sectors or international organisations,

(ii) Presence of the following appropriate safeguards in the absence of the Board's adequacy decision;

- Existence of an agreement that is not of international agreement nature and the Board's approval,
- Existence of binding corporate rules and the Board's approval,
- Signing the standard contractual clauses published by the Board and notification to the Board or
- Executing a commitment between the transferer parties to ensure adequate protection and Board's approval

Signing standard contractual clauses is not sufficient to fulfill legal obligations for cross-border data transfer. Both data controllers and data processors need to notify the signing of the standard contractual clause to the Board within five days. Failure to notify within this period may result in administrative fines ranging from TRY 50,000 to TRY 1,000,000 for both the data controllers and the data processors. While standard contractual clauses have not yet been published by the Board, a comprehensive regulation for cross-border data transfer is expected to enter into force soon.

The Amendment Law also regulates the rules of incidental and nonrepetitive cross-border data transfers. However, these rules are applicable only for exceptional circumstances. Transferring personal data abroad based on explicit consent legal ground is indicated for incidental and nonrepetitive cross-border data transfer. Besides, the Amendment Law also specifies that the rules regarding cross-border data of transfer of PDPL are applicable for onward transfers.

3. Appeal Process Against the Board Decisions

The Amendment Law stipulates that appeal proceedings against decisions made by the Board will now fall under the jurisdiction of the administrative courts rather than criminal courts of peace. This amendment ensures that Board decisions undergo scrutiny by a specialized court, allowing for a more thorough review of their merits.

The Amendment Law will enter into effect on 1 June 2024. However, the existing provisions concerning cross-border data transfer, along with the amendments, will remain in force until 1

September 2024. Therefore, data controllers are required to ensure compliance with the new amendments within this timeframe. It is also important for data controllers to closely adhere to the forthcoming comprehensive secondary regulations to ensure compliance with the rules regarding cross-border data transfer.

CONTACT

Maral Minasyan
mminasyan@kolcuoglu.av.tr

Bahar Esentürk
besenturk@kolcuoglu.av.tr