Data. Protection. Adding Value.

Data Protection Laws - Turkey

Legislation

Data privacy in Turkey is primarily governed by the Law on Protection of Personal Data No. 6698 ("**PDPL**"), which is influenced by the European Union's data protection regime and aims to protect the fundamental rights and freedoms of individuals in the processing of personal data. Additionally, the Turkish Criminal Code ("**TCC**") contains specific articles that address violations related to personal data.

Scope: The PDPL does not include a provision on territorial scope. Nonetheless, rulings from the Turkish Data Protection Authority clarify that a data controller, even if not based in Turkey, may come within the jurisdiction of the PDPL if it processes the personal data of Turkish nationals or residents.

Exemptions: The PDPL governs the protection of personal data pertaining exclusively to natural persons, excluding data unrelated to filing systems or used solely for personal or familial activities, provided it remains undisclosed to third parties. Further exemptions apply to anonymized data utilized for official statistics, data processed for artistic, scientific, or expressive purposes, and data managed by authorized public, judicial, or intelligence bodies.

Risk Level: High

Supervisory Authority

Supervisory Authority: The Turkish Data Protection Authority ("**DPA**") is a public legal entity with administrative and financial autonomy. The DPA's primary role is to enforce data protection laws, monitor developments, and collaborate with national and international bodies.

Registration/Approval Requirements: Data controllers are required to enroll in the Data Controllers Registry System ("**VERBIS**"), managed by the DPA, and must upload their data inventories prior to initiating data processing activities. Exceptions to this mandate include professional entities such as legal professionals, notaries, and accountants, along with political parties, trade unions, and small data controllers who engage minimally in sensitive data processing. Additionally, certain data processing actions, such as those related to crime prevention, data publicly disclosed by the subject, regulatory functions, and protection of Turkey's financial interests, are also exempt from registration.

General Data Privacy Principles

The procedures and principles regarding the processing of personal data in the PDPL are regulated in accordance with the Convention No. 108 and the European Union Directive No. 95/46/EC. As such, the general principles listed in the PDPL are as follow:

- **Lawfulness and fairness**: Personal data must be processed lawfully, fairly and in a transparent manner.
- **Accuracy**: It must be ensured that the personal data is accurate and up-to-date.
- **Purpose limitation**: Personal data may only be processed for a specified and legitimate purpose, and not processed in a manner that is incompatible with those purposes.
- **Data minimisation**: Processing must be relevant and limited to what is strictly necessary to achieve the processing purposes.
- **Storage limitation**: Personal data must only be stored as long as it necessarily required for the processing purpose, incl. applicable retention obligations. Personal data should not be kept for longer than is necessary for the purposes for which the personal data are processed. There must be specific retention periods after which the information should be deleted or anonymized.

Enforcement

The DPDPA allows for the following fines to be issued:

Non-compliance with the obligation to register and notify the Data Controllers Registry	**TRY 272,380** to **TRY 13,620,042**
Non-compliance with the decisions of the Board	**TRY 340,476** to **TRY 13,620,402**
Non-compliance with transfer obligations	**TRY 71,965** to **TRY 1,439,300**
Non-compliance with data security obligations	**TRY 204,285** to **TRY 13,620,402**
Non-compliance with information obligations	**TRY 68,083** to **TRY 1,362,021**

Furthermore, the TCC Outlines various criminal offences, including **unlawful recording, acquisition, or dissemination of personal data**, reinforcing legal protections against data privacy violations and ensuring accountability for breaches.

Data Processing

The Legal Basis for Processing: The primary basis is explicit consent of the data subject. However, it is not necessary to obtain explicit consent where processing is: (i) explicitly provided for by law; (ii) necessary for the protection of life or physical integrity and the individual cannot provide consent; (iii) relates to the personal data of the parties to an agreement and is directly related to the conclusion and/or fulfilment of the agreement; (iv) mandatory for the data controller to fulfil its legal obligations; (v) made manifestly public by the data subject; (vi) necessary for the establishment, exercise or protection of a right; or (vii) required for the legitimate interests of the data controller and does not violate the fundamental rights and freedoms of the data subjects.

Sensitive Personal Data: Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data are deemed to be special categories of personal data.

Transparency Requirements

Transparency obligations are fulfilled through explicit **privacy notices**, which must include the identity of the data controller, the purpose of processing of personal data, to whom and for which purposes the processed personal data may be transferred, the method and legal basis of collection of personal data, and the rights of the data subject.

Fulfilment of the obligation to inform does not depend on the request of data subject.

pwc

Data Subjects Rights

Data Subjects have the following rights under Article 11 of the PDPL in relation to the processing of their personal data:

- **Right to access personal data**
- **Right to correction of personal data**
- **Right to be forgotten and erasure of personal data**
- **Right to notification of third parties processing personal data.**
- **Right to object to results based solely on automated processing of personal data.**
- **Right to damages caused by unlawful processing of personal data.**

It is obligatory for data subjects to apply to the data controller in order to exercise their rights. A complaint cannot be made to the Board before this remedy is exhausted.

Security & Data Breaches

Security Requirements: Data controllers are mandated to implement necessary technical and organizational security measures to prevent unlawful processing and access, and ensure data protection.

The DPA has also rendered decision No. 2018/10 requiring entities or individuals processing special categories of personal data to implement supplementary protective measures to safeguard any sensitive personal data they handle.

Data Breaches: In the event of a data breach, controllers must notify the DPA within 72 hours after becoming aware.

Notification to individuals affected by the breach should be made without undue delay, using direct or indirect methods such as website announcements. Data controllers are also required to document all breaches, detailing the incident, its effects, and remedial actions taken, for review by the DPA.

Other Business Obligations

The Turkish Personal DPA's decision no. 2018/10 mandates strict security measures for data controllers handling sensitive personal data, including:

1. Develop and maintain a clear **policy and procedures** for the processing and security of sensitive personal data.
2. **Train employees** in data security, enforce confidentiality agreements, and manage access rights efficiently.
3. Utilize **cryptographic methods** for data storage and access, maintain **security protocols**, and ensure **multi-factor authentication** for remote access.
4. Implement adequate **physical security measures** to protect data environments from various risks.
5. Securely **transfer data using encryption methods**, including encrypted emails via corporate or Registered Electronic Mail accounts.
6. Follow the **technical and administrative guidelines** outlined in the Personal Data Security Guide on the Authority's website.

Cross-Border Transfers

Cross-Border Data Transfers: Under the PDPL Law Amendments, the regime for international data transfers includes:

(i) Adequacy Decisions: Maintained as a valid legal basis, now extended to include international organizations and specific sectors within third countries, enabling the DPA to issue decisions accordingly**.**

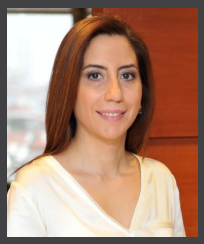
(ii) Appropriate Safeguards: Transfers without adequacy decisions require safeguards such as Binding Corporate Rules (BCR), Standard Contractual Clauses (SCCs), agreements between institutions (with DPA approval), or written undertakings providing adequate protection.

(iii) Occasional Transfers: If a transfer does not meet the criteria for adequacy decisions or appropriate safeguards, it can still proceed under specific conditions such as necessity for contract performance, overriding public interests, or with explicit consent from the data subject, provided the transfer is non-repetitive and informed consent about potential risks has been obtained.

To Watch

Localization Requirements: While the PDPL does not impose explicit data localization requirements, the transfer of personal data outside of Turkey is regulated stringently, requiring adherence to specific conditions ensuring adequate protection or appropriate safeguards, which may influence decisions regarding data localization to simplify compliance.

Let's connect to discuss how we can help:



Ezgi Türkmen
Head of Legal Services
Partner, PwC Turkey

+90 (533) 457 8626
ezgi.turkmen@pwc.com

This publication has been prepared for general guidance on matters of interest only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2025 PwC. All rights reserved. Not for further distribution without the permission of PwC. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details