MOROĞLU ARSEVEN

Turkey Completes Final Step in Approving Data Protection Legislation

7 Apr 2016

Turkey has completed the final step in a long running process to enact the Data Protection Law number 6698 ("**Law**"). The Law referred to in our recent article has now received Presidential approval and its final text was published in Official Gazette number 29677 on 7 April 2016.

From 7 April 2016 onward, a general prohibition now applies in Turkey on processing or storing personal data without express consent. The Law addresses responsibilities of key actors, companies and data processing companies, as well as appropriate methods for processing and transmitting data. It creates a relatively similar framework to the European data protection system, although there are areas of difference which can be found in our previous article.

Key definitions:

Significant definitions introduced by the Law include:

- "*Personal Data*", meaning any information relating to an identified or identifiable living individual.
- "*Sensitive Data*", a type of Personal Data, which receives extra protection. It is defined as information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, appearance, memberships of unions, associations or foundations, as well as information about health, sexual life, criminal records, punitive measures, as well as biometric and genetic data.

The Law proposes extra processing obligations for sensitive data. Therefore, any requirements under the Law for personal data would also apply to the sensitive data category defined above.

The Law introduces a general prohibition on processing personal or sensitive data without express consent. However, it does not clarify how express content should be obtained. In light of this, companies would be prudent to both record and retain consents, either in writing or electronically.

Transition into the new data protection regime:

Under the Law, the following steps will apply for introducing the new requirements for processing personal data in Turkey.

1. From 7 April 2016 onward:

All companies collecting personal data in Turkey must now take the following measures:

- Obtain express consent before collecting new personal and sensitive data.

- Survey data which was collected before the Law was enacted.
- Designate an authorized staff member to carry out the operations in respect to data protection.
- Establish a control system for data protection and regularly audit the system.
- Create a customized compliance strategy with professional help.

2. Register with the Data Controller Registry:

Once the Data Protection Board ("**Board**") is established and the Data Controller Registry begins operations, data controllers must apply for registration. Applications must include certain information, including classification of the personal data, purpose for processing data, data subjects, parties whom the data is transferred to, the country the data is transferred to, as well as the processing period.

3. Transferring data outside Turkey, or to third parties:

The Law addresses transmission of personal data to third parties, as well as transmissions outside Turkey. This is particularly relevant for multinational companies and local companies, which have operations which cross Turkey's national borders. Companies should review their operations to ensure they are aware where personal data is stored and whether the new legislative rules will apply. Data transfer requirements under the Law will apply from 7 October 2016 onward.

The Law requires express consent from data subjects for:

- *Transfers to third parties*. Consent will not be required if the transfer is necessary to exercise a right, is required by law, or the data is public.
- *Transfers outside Turkey*. Consent will not be required if the transfer is necessary to exercise a right or is required by law, and either:
    - Sufficient protection exists in the transferee country, or
    - If there is no sufficient protection exists in the transferee country, if the data controller gives a written security undertaking and the Board grants permission.

When granting permissions, the Board must evaluate international treaties, reciprocity of countries, measures taken by the data controller, as well as the period and purpose of the data processing.

4. Ensure existing data meets the Law's requirements within two years:

Data which qualifies as "personal data" (including sensitive data) but was collected before 7 April 2016, must become compliant with the Law's requirements by 7 April 2018 (two years from the enforcement date).

5. Ongoing obligations for data controller:

After the Board approves and registers a data controller, it (or related data processors) must:

- Inform and notify data subjects about processing personal data.
- Store personal data.

- Prevent unlawful processing and access to personal data.
- Comply with technical and administrative measures and supervisions.

Milestone dates:

Persons or companies which store or process personal data should pay attention for further developments on this topic in the near future.

Key milestone dates are:

- **7 April 2016**: The Law's enforcement date (with certain exceptions). Obligations apply from this date forward for collecting new personal data.
- **7 October 2016** (six months after the enforcement date):
    - Deadline for establishing the Data Protection Board and Data Controller Registry.
    - Data Controllers must be registered with the Data Controller Registry from this date onward and the deadline for such registry will be determined by the Data Protection Board.
    - The following obligations will apply once the Data Protection Board and Data Controller Registry are established:
    - Provisions regarding data transfers to third parties and abroad.
    - Data subjects can exercise their rights against the Data Controllers and the Data Controller Registry (for example, access information, request data be deleted, or make complaints).
    - Procedures and principles for complaints to the Board by data subjects.
    - Criminal offenses and punitive measures for failure to comply with the Law.
- **7 April 2017** (12 months after the enforcement date): The deadline for secondary legislation to be enacted, likely including further details about operational processes and procedures.
- **7 April 2018** (two years after the enforcement date): The deadline for ensuring all data already collected prior to the Law's enforcement date is compliant. Personal data which has not met the compliance criteria by this date must be immediately anonymized or erased.

Please see this link for full text of the Law (only available in Turkish).

Related Practices

- Privacy and Data Protection