MOROĞLU ARSEVEN

Turkey Adopts Data Protection Law, Taking a Big Step Towards Harmonization With Relevant Elements of Acquis Communautaire

24 Mar 2016

After more than a decade of legislative proposals, the Grand National Assembly of Turkey has approved the Data Protection Law ("**Law**"). The next step is for the new law to receive approval or comments from Turkey's President, then eventually be published in the Official Gazette with the official text and an enforcement date. The Law addresses responsibilities of key actors, companies and data processing companies, as well as appropriate methods for processing and transmitting data. It introduces definitions for "Personal Data", "Sensitive Data", "Data Processor", "Data Controller" and "Explicit Consent", among others, as well as a general prohibition on processing or storing such data without express consent from the data subject. For personal data which is already stored or begun processing before the Law's enforcement date, data processors and data controllers have two years to ensure the data complies with the new requirements.

The Ministry of Justice of Turkey submitted the Data Protection Law to the Council of Ministers on 18 January 2016. The Assembly approved the Law on 24 March 2016, with some changes relating to transferring data outside Turkey and the election process for the Data Protection Authority. The next step in the enactment process is for the new law to receive approval from Turkey's President and to be published in the Official Gazette, with the official text and an enforcement date. Secondary legislation should be enacted within one year of the Law's enforcement date.

The Law outlines a relatively similar framework to the European data protection system. However, further changes are necessary if Turkish legislation is to become completely aligned with the European Union's data protection regime.

Significant aspects introduced by the Law include:

- A range of definitions, including notably:
    - "Personal Data", meaning any information relating to an identified or identifiable living
    - "Sensitive Data", a sub-set of Personal Data, which is subject to certain extra 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 and biometric data.
    - Data Controller", "Data Processor" and "Data Controller Registry" are defined, although a different approach to European Union legislation has been accepted.
    - "Explicit consent" is defined.
    - "Anonymization" is introduced.

- Processing Personal or Sensitive data without express consent is prohibited. Notably, the Draft Law is silent on how such consent should be obtained. Therefore, companies would be prudent to record and store consents in writing and/or electronically.
- The difference between data controller and data processor is clarified, along with respective obligations. Data controllers must register with the newly established Data Controller Registry, even before they begin to actively process data. The registry will be launched following establishment of the Data Protection Board, within six months of the Law's enforcement date.
- The Law will be enforceable as from the publication date in the Official Gazette. Therefore, the Law's requirements will apply immediately for collecting and storing new personal data. An exception is the obligation register with the Data Controller Registry. The registry will be launched following establishment of the Data Protection Board, within six months of the Law's enforcement date.
- Personal data which is already collected or stored before the Law's enforcement date must become compliant with the new requirements within two years. If the data is not compliant at that time, it must be deleted or anonymized.
- Persons or companies which collect or store personal data must comply with technical and administrative measures and supervisions.

Procedures for transferring data outside Turkey or to third parties are clarified, along with limited exceptions where express consent is not necessary.

A legislative structure and definition is introduced for Turkey's national data protection authority: the Data Protection Authority and Data Protection Board. The Data Protection Authority will include the Data Protection Board and the Board's President.

The Data Protection Board will be established within six months of the legislation being published. Out of nine proposed Authority members, two would be appointed by the Council of Ministers, while two would directly be appointed by Turkey's President. The remaining five member will be elected by the Turkish Parliament.

Therefore, persons or companies which store or process personal data should pay attention for further developments on this topic in the near future. Key milestones are:

- Publication in the Official Gazette and enforcement date (the Law's obligations will apply for new data from this date onward and this date will be the basis for measuring other milestones).
- Six months after enforcement (deadline for launch of the Data Controller Registry).
- 12 months after enforcement (deadline for secondary legislation).
- Two years after enforcement (deadline for ensuring all data already collected prior to the Law's enforcement date is compliant).

Related Practices

- Privacy and Data Protection