Data Protection Issues in Turkey

Begüm Yavuzdogan Okumus, managing associate of Gun+Partners, looks at the impact and improvements the GDPR will have on Turkish data protection

In April 2016, Turkey faced one of the biggest data breaches ever recorded, where it was claimed that the personal data of almost 50 million Turkish citizens was leaked online. That breach is currently being investigated by the prosecuting officer, and although officials claim that the data leak only contains data from 2009 and reveals no new records beyond that time – it is still accepted as a colossal data breach.

In the meantime, the long awaited Data Protection Law (the "Law") entered into force on 7 April 2016, just days after the news of Turkey's biggest data breach. For many years, Turkey had lacked a separate legislative measure regarding the issue of data protection. Previous draft laws that had been sent to the Turkish Parliament were either returned to the proposing committee or not even discussed. Adoption of data protection law was a real need both for the Turkish society and for Turkey's harmonization with EU regulations.

The Law contains detailed provisions relating to the protection of personal data, an area that was previously only covered by an insufficient and piecemeal application of different legislative measures and the Turkish Constitution.

The Law introduces an official definition for the term *"personal data"*, defining it as "any type of information that relates to an identified or identifiable natural person". This means that the Law covers data of real people and its scope is very wide indeed. The main principle is that personal data can only be processed once the data subject has provided explicit consent. However, personal data can be processed without obtaining explicit consent in cases of certain exceptions stated under the Law.

The Law also separately distinguished a category of *"personal data of a special nature"* which is subject to a more extensive level of protection. The types of personal data that fall under this category are related to race, ethnicity, political views, philosophical belief, religious denomination or other beliefs, clothing and attire, membership in associations, charities or trade unions, health, sex life, convictions, security measures and biometric data. The law-maker has set the standard of prohibition of processing personal data of special nature, unless explicit consent of the data subject is present.

It must be noted that health and sex life data cannot be processed in any case without an explicit consent and even in the presence of explicit consent, such data can only be processed by persons or authorized institutes bound by the duty of confidentiality for the purpose of the protection of public health, the provision of medical, diagnostic and treatment services and the planning, managements and financing of healthcare services.

The Law further provides for data security obligations for data controllers and stipulates that data controllers are under the obligation to implement all kinds of technical and administrative measures to maintain a security level that would avoid unlawful processing of and access to personal data, whilst also safeguarding personal data. The data controller and data processor are *jointly liable* for maintaining the security measures under the Law.

It should also be noted that the data controller has a duty to inform the Data Protection Board and the relevant party if and when personal data has been unlawfully accessed. Thereafter, the board has the discretion to announce the breach on its website or another via another communications channel.

In addition to criminal sanctions stipulated under the Turkish Criminal Code and repeated under the Law, the Law introduces monetary sanctions. Data controllers will face administrative monetary sanctions between the range of TRY 5,000 (approx. EUR 1,500) and TRY 1,000,000 (approx. EUR 300,000) if they are in breach of their obligations to inform the data subject, to ensure data security, enforce the decisions of the board and to the register.

Under the Law, there is a transition period of two years for data controllers to make personal data that has been processed prior to the enactment of the Law in compliance with the Law. In case such compliance is not ensured, incompliant personal data will be deleted, destroyed or anonymized.