COSMOS
Navigate the Compliance Universe

Report on Supply Chain Compliance Volume 3, Number 22. November 12, 2020
Turkish data protection authorities fine Twitter and Facebook

By Sascha Matuszak

Turkish authorities recently fined[1] Twitter, Facebook and several other social media platforms for failing to appoint a country representative in accordance with Turkey's Data Protection Law.

According to the law, first published in April 2016, data processors had until Nov. 2 to appoint country representatives; Twitter, Facebook, Instagram, Periscope and TikTok have each been fined 10 million Turkish lira, equivalent to USD 1.2 million, for missing the deadline. None of the companies commented on the fines.

If the companies fail to pay the fines or appoint a country representative, they face an escalating series of enforcement actions that could culminate in restriction of services and access to the Turkish market.

Not a new law

Turkish authorities have been clarifying areas of the law, releasing decisions on jurisdiction and exemptions, imposing fines on violators, and refining the scope of the law since April 2016. For example, the Data Protection Board:[2]

- "Declared that data controllers must prepare a separate policy and procedure for protecting special categories of personal data" in 2018;
- "Declared that entities providing services at service counters, box-offices, and desks must ensure that only authorised persons are in these locations, as well as take necessary measures to prevent people receiving services at these locations from seeing or hearing each other's personal data";
- "Found that websites and applications which offer phone directory services (searchable via phone number or name) and share personal data without any justifiable reason determined under the Data Protection Law and relevant legislation, must immediately cease their activities or face either administrative or criminal sanctions."

The board has also made numerous summaries and decisions regarding everything from registration deadlines to cross-border data transfers. Some of the fines imposed include:

- A newspaper that disclosed personal data without obtaining explicit consent.
- A fine imposed on Facebook for more than USD 200,000 for failing to take necessary technical and administrative measures to prevent data breaches and failure to notify the board of the breach.
- "An asset management company that sent text messages to a data subject on multiple occasions regarding the same issue without obtaining...explicit consent."

The law also has specific requirements on the storage of personal data from Turkish sources and the cross-border transfer of personal data.

According to the law,[3] both nonsensitive and sensitive personal data can be transferred outside Turkey based on any of their respective processing grounds, as long as the data subject provides explicit consent. If the data controller is transferring data and processing data under grounds that do not require explicit consent, such as the data are not sensitive personal data, the Turkish Data Protection Law stipulates that:

- "The destination country must have an adequate level of protection, which is to be determined by the DPB; or
- "Both sides of the transfer must commit, in writing, to provide an adequate level of protection and the approval of the DPB must be obtained."

Additionally, the DPL authorizes the Data Protection Board to halt cross-border transfers in the interest of Turkey:

"'Save for the provisions of international agreements, in cases where interests of Turkey or the data subject will be seriously harmed, personal data shall only be transferred abroad upon the approval of the Board by obtaining the opinion of relevant public institutions and organizations.'"

This measure seems to hold controllers liable for cross-border transfers that harm Turkey's interests and places the responsibility on controllers to obtain an opinion from the board before transferring data. This clause was criticized by businesses who claimed it put too much of a burden on companies to determine what is and is not in the interests of Turkey.

Turkey's data protection law is modeled after the GDPR and contains similar language. There are specific regulations that are individual to Turkey (e.g., the "Turkish interests" clause), but the law is part of a wave of data protection legislation sweeping across the world in the last five years.