

Data Protection Rules in Turkey – What Next?

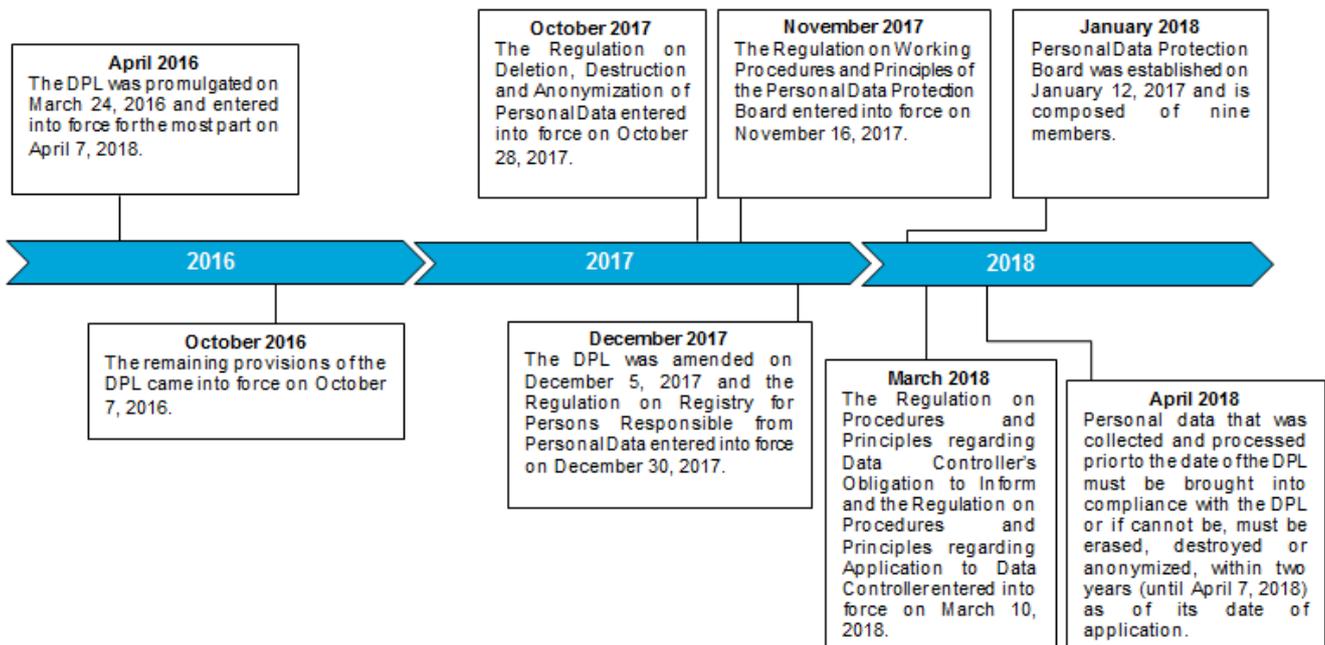
May 2018

Authors: [Ceylan Kara](#), [Emre Özşar](#), [Aslı Gülüm](#)

Turkey's first Data Protection Law ("DPL") came into force for the most part in April 2016. However, certain important provisions came into force later or were introduced by the regulations under the DPL published in late 2017.

In this alert, we will remind you of the major developments introduced by the DPL and the actions that you should have taken or should be taking to comply with the DPL and the regulations published pursuant to the DPL (together, the "DPL Laws").

Here is a timeline of the developments to date in data protection in Turkey:



To recap what you should have done to date:

- Determined whether your company is “Processing Personal Data”: given the broad scope of the relevant definitions, the answer is likely to be “yes”.
 - **Personal Data** is defined in the DPL to include any and all kinds of information relating to an identified or identifiable real person; and
 - **Processing** is defined to include all acts performed on this Personal Data including collection, recording, storage, retention, alternation, disclosure, re-organization, disclosure, classification etc. – whether fully or partially through automatic or non-automatic means.
- Sought express consent from your data subjects: the DPL’s guiding principle is that Personal Data cannot be processed without the “express consent” of the data subject.

So, if you are processing Personal Data, you should have sought the express (written) consent of your data subjects by informing them of:

- their rights under the DPL;
 - relevant matters under the DPL Laws, including the proposed use of the data, any possible transfer and the legal basis for collection of the Personal Data; and
 - the identity of the data controller in your company – you should have appointed this person under the DPL Laws.
- Assigned and registered in the data controllers’ registry a data controller in the meaning of the DPL and empowered and assisted the data controller to take “all necessary technical and organizational measures” to meet the requirements of the DPL. These measures must permit the data controller to carry out the obligations in respect of (i) informing data subjects of their rights and of the company’s processing of their Personal Data and (ii) taking measures to ensure data security.
 - Become compliant by April 7, 2018 with the DPL for Personal Data that you have collected and processed before the publication of the DPL. This means that:
 - you should have sought express consent from the data subject of such data or; if you have not, or the data subject has not consented, then
 - you should have erased, destroyed or anonymized such data prior to such date.
 - Considered whether your company is processing any of the special categories of Personal Data for which the DPL has separate and more stringent requirements (such as health; or race, religion, personal conduct and other similar categories) and comply with those requirements; and
 - Finally, and most importantly, ensured that you are now collecting and processing Personal Data in the manner required by the DPL, including:
 - fairly and legally;
 - for limited use and not excessively;
 - accurately and up to date; and
 - securely.

What has the Board for Protection of Personal Data (the “Board”) done and what can you expect from them?

- The Board has been constituted and has nine members.
- The duties and powers of the Board includes to:
 - ensure that Personal Data are processed in accordance with fundamental rights and freedoms;
 - take final decisions with respect to complaints made to the Board that rights relating to Personal Data have been violated;
 - impose the administrative sanctions prescribed by the DPL Laws;
 - take other necessary regulatory actions; and
 - determine what will be the adequate security measures required for processing special categories of Personal Data.
- The Board has already issued three decisions one of which is based on Article 6(4) of the DPL and determines what are the adequate security measures that data controllers must take when processing special categories of Personal Data (e.g. relating to race, political, religious, health conditions and the like).

What if I wish to transfer Personal Data outside of Turkey?

- You must have express consent from the data subject to transfer.
- The receiving country must have sufficient legal protection in place or, if it does not, the data controller in the receiving country must undertake to protect the data and you must receive Board consent.
- As to Personal Data transfers to EU countries, the EU General Data Protection Regulation (GDPR) will apply starting on May 25, 2018 and offers sufficient protection.

What are the sanctions for failure to comply with the DPL Laws?

- The DPL imposes criminal sanctions stipulated under the Turkish Criminal Code for some breaches under the DPL; this can mean sentences from one to two years under the relevant provisions of the Turkish Criminal Code.
- The DPL also imposes administrative sanctions (fines of TL 5,942 – TL 1,188,542 or approximately \$1,485 to \$297,135 at current exchange rates) on violation of certain provisions of the DPL and these can apply to real and legal persons who are data controllers. It is not clear whether these will apply per breach or whether they will apply at the upper limit for all breaches by the same person.
- Publicly-available information shows that there were 41 applications made to the Board in 2017 alleging breaches in sectors including media, banking, health and insurance. Nineteen of them were finalized and administrative fines were imposed on companies.

Conclusion

- The DPL Laws represent a big step forward in the protection of the rights of Turkish citizens with respect to their Personal Data and towards harmonization with the EU GDPR.
- Implementation of the DPL Laws will remain a work in progress for some time and many questions remain. The Board has already issued a number of decisions and clarifications that address some of the frequently-asked questions about implementation and seems committed to continuing to guiding companies to take the right steps in respect of protection of Personal Data.

GKC Partners

Maya Akar Center

Büyükdere Caddesi No: 102 Kat: 28

34394 - Esentepe, Istanbul – Turkey

T +90 212 355 13 00

This information is provided for your convenience and does not constitute legal advice. It is prepared for the general information of our clients and other interested persons. This should not be acted upon in any specific situation without appropriate legal advice and it may include links to websites other than the website.

GKC Partners has no responsibility for any websites other than its own and does not endorse the information, content, presentation or accuracy, or make any warranty, express or implied, regarding any other website.

This information is protected by copyright and may not be reproduced or translated without the prior written permission of GKC Partners.