MOROĞLU ARSEVEN

# What you need to know when the Board comes knocking at your door?

*11 Nov 2020*

Article 15 of Turkey's Law on Protection of Personal Data No. 6698 ('LPPD') allows the Personal Data Protection Board ('the Board') - the decision-making authority within the Personal Data Protection Authority ('KVKK') - to carry out investigations on its own initiative, or when it receives complaints. However, unlike the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), the LPPD does specify the regulator's powers. Burcu Tuzcu Ersin and Ceylan Necipo?lu, Partner and Senior Associate respectively at Moroglu Arseven Avukatl?k Ortakl???, take us through every key aspect of the Board's investigatory and enforcement powers, from how and why the Board may conduct investigations to the appellate mechanisms available to data controllers subject to the Board's decisions.

## Launching investigations

The Board can initiate surveillance and legality monitoring investigations either *ex officio* or as a result of a data subject's complaint.

*Ex officio* investigations may be conducted based on information provided by the supervisory body, public authority, data subject, employee of a data controller (e.g. whistleblowers), or third parties. In GDPR practice, data controllers are audited by independent auditors in certain periods and the audit reports are sent to the data protection authority of the relevant country. Data protection authorities may initiate an investigation relying on these audit reports. Contrary to the GDPR, the Board has no possibility to start an investigation by relying on such audit reports, since no data protection audit report mechanism is regulated under the LPPD. The Board may become aware of an infringement by the information on press releases, news, social media posts, market researches, or even information obtained during a continuing investigation and decide to conduct an *ex officio* investigation.

Apart from *ex officio* investigations, investigations following a complaint may be initiated by the Board as a result of the receipt of a complaint from data subject about a potential violation of the LPPD. Data subjects whose rights are violated are allowed under the LPPD to file a complaint with the Board if certain conditions are fulfilled. In principle, in order to be able to file a complaint with the Board, an initial application to a data controller must be made by data subjects. According to the LPPD, the data subject may file a complaint with the Board within 30 days of the receipt of responses and, in any case, within 60 days of the date that controllers were approached, in the following circumstances:

- the application is declined by data controller;
- the response given by data controller is found unsatisfactory; or
- the response is not given in due time by data controller.

The Board will only consider complaints if they fit the following requirements as prescribed by Article 6 of the Law on the Exercise of the Right to Petition No. 3071 ('Law No. 3071'):

- complaints must contain a concrete claim and the purpose of and final request in the petition must not be ambiguous;

- the subject of complaints must not fall within courts' exclusive jurisdiction (such as compensation claims or criminal justice requests); and
- the required information stated in Article 4 of Law No. 3071 must be provided.

When a complaint covering the above requirements is duly filed, it will be examined by the Board, and the Board can decide to initiate an investigation against data controllers or can decide to decline the complaint. If complainants do not receive an affirmative or negative respond within 60 days from the Board informing them that their complaints have been dismissed, complaints are deemed to be declined without any further notice. Complainants can approach administrative courts to review decisions to dismiss complaints.

# Scope and limits of the Board's authority

The Board's investigative authority is vested under Article 15 of the LPPD, though without any attributions clarifying specific extent or limit. Article 15(3) of the LPPD sets forth that data controller shall, within 15 days upon notice, deliver to the Board all information and documents, except for those qualifying as state secrets. Obviously, the Board's investigative authority under this clause finds its limit under Article 22 of the LPPD, which sets forth the authorities of the Board. Furthermore, the authority of the board should be, save for the restrictions arising from the Constitution and basic principles of administrative law, interpreted only as broadly as the specific circumstances of the incident at hand require. If the same results can be achieved as effectively by using less public force, the use of exceeding public force cannot be regarded as proportional and therefore lawful. The Board would indeed be expected to use its authorities in the same manner as would be expected from any administrative authority under the general principles of Turkish administrative law and should always adhere to the principle of lawfulness, fairness, proportionality and transparency.

Unlike GDPR, the territorial scope of the LPPD is not explicitly stipulated. In the absence of such territorial scope, the applicability of the LPPD and whether the Board would have jurisdiction on any specific incident shall be evaluated based on the sanctions that are attributed to each such incident. Article 18 provides the misdemeanours related to the violation of the law. Therefore, in each case where the Board uses its investigative authority, the assessment should be made on the basis of the application rules based on territory under the Misdemeanors Law No. 5326 ('the Misdemeanors Law'), which addresses the topic to the Turkish Criminal Code's related provisions. In case the incident is determined to fall within the scope of the territorial scope of the LPPD, the Board would have the authority to investigate the incident, reach a decision and enforce the given decision regardless of data controller having its registered address in Turkey or in abroad.

# Investigation methods

As and when an investigation is initiated as explained above, all necessary information in respect of the incident starts to be gathered by the Board. In this manner, the investigation methodology will be determined by considering how the necessary information can be acquired. Unlike other independent supervisory authorities, the Board's investigative authorities are not regulated in a detailed manner in the LPPD.

On-file investigations are conducted on the base of a notification letter sent to data controller whereby the Board requests information and documents needed to resolve the case. Article 15(3) of the LPPD sets forth that data controller shall, within 15 days upon notice, deliver to the Board all information and documents, except for those qualifying as state secrets.

In case a need for an on-site inspection emerges before or during an investigation in order to gather the required information to conclude, an on-site inspection can be conducted by the Board. The Board is not under the obligation to notify data controllers before an on-site inspection takes place. In other words, the Board is entitled to initiate a spontaneous on-site inspection without signalling or notifying the data controller in advance. Authorised officers can conduct a full-scale inspection at the data controller's premises, on all information systems and documents by

capturing disk and/or servers or walking-through on the information systems.

The data controller is obliged to enable on-site inspection and provide all information requested within the authority of the Board. In case the Board's information and document requests, which are made on the grounds of an initial decision of the Board for launching the investigation, are not satisfied, an administrative fine can be imposed on data controller as prescribed by Article 18(3) of the LPPD.

By taking into consideration all information, documents, evidence and defence letter provided by the data controller under the investigation made upon complaint or *ex officio*, the Board can either decide on the existence of infringement or decide to decline the complaint if no infringement can be detected.

In case an infringement is determined by the Board, it shall;

- notify the data controller and deliver the reasoned decision;
- publish the decision if it has the quality of a principle decision;
- if the measures decided upon by the Board are not completed by the data controller, impose an additional administrative fine for the nob-compliance with the Board's decision;
- decide that processing of data or its transfer abroad should be stopped if such operation may lead to damages that are difficult or impossible to recover and if it is unlawful.

# Board decisions

The administrative fines that the Board is authorised to impose on data controllers are determined under Article 18 of the LPPD. Accordingly, the Board is authorised to impose:

- an administrative fine of TRY 9,013 to TRY 180,264 (approx. €970 to €19,400) on those who fail to comply with the obligation to inform provided for in Article 10 of the LPPD;
- an administrative fine of TRY 27,040 to TRY 1,802,636 (approx. €2,910 to €194,000) on those who fail to comply with obligations related to data security provided for in Article 12 of the LPPD;
- an administrative fine of TRY 45,066 to TRY 1,802,636 (approx. €4,850 to € 194,000) on those who fail to comply with the decisions issued by the Board under Article 15 of the LPPD; and
- an administrative fine of TRY 36,053 to TRY 1,802,636 (approx. €3,880 to €194,000) on those who fail to meet the obligations for enrolling in the Registry of Data Controllers ('VERBIS') and making a notification as provided for in Article 16 of the LPPD.

Separate administrative fines can be imposed for each item above. The gap between the minimum and maximum amount of fine is intentionally kept broad in the LPPD, so it is possible to say that the amount of the fine is at the Board's discretion, which shall be given in line with the general principles of Turkish Law. In particular, as required under Article 17(2) of the Misdemeanors Law, the Board shall decide on the weight of sanction in each case upon its evaluation of:

- type of infringement;
- how severe it was and how long it lasted;
- whether it was deliberate or accidental;
- actions taken to reduce the damage to data subjects; and
- the security measures taken by data controllers.

In this manner, the same infringement made by different data controllers may be fined by the Board differently due to these variables.

Following the examination made upon complaint or *ex officio* investigation, in cases where it is understood that an infringement exists, the Board shall decide that the identified infringements shall be remedied by the relevant data controller. As and when an infringement is detected by the Board, the measures decided by the Board for the remedy

of the infringement should be completed by the data controller within 30 days after the notification to the data controller as per Article 15(5) of the LPPD. If not, the Board is also authorised to decide for a cessation of data processing or cessation of the data to be transferred abroad as per Article 15(7) of the LPPD.

# Notification and publication of the Board's decisions

As a rule, the Board's decisions shall be notified to data controllers. In case the data controller is a legal person incorporated under Turkish laws, notification has to be made electronically to the e-notification address of the data controller as per the Electronic Notification Regulation. The decision is deemed to be notified to the data controller at the end of the fifth day following delivery of e-notification to the e-notification account of the data controller regardless of being read by data controller or not. Therefore, data controllers are obliged to check the e-notification accounts for new e-notifications regularly. If electronic notification cannot be made for an act of god, a decision can be delivered to the data controller in a traditional manner by the post.

If the data controller's registered address is in Turkey, the decision is delivered to the data controller according to the local laws. However, if the data controller's registered address is in another country, the international notification procedure should be applied. In general, the decisions of the Board are just delivered to the related data controller since the Board is not following the transparency principle which means that Board decisions are not publicly available. The Board, however, may publish the decision under Article 15(6) of the LPPD, if the occurred infringement subject to the decision becomes widespread among the data controllers.

Finally, it should be noted that the Board's decisions are not limited to those given upon an investigation. The Board is authorised to publish principle decisions concerning all data controllers, data processors, and data subjects for regulating data processing activities. Principle decisions are binding for all data controllers and they are expected to alter their operations in accordance with the principle decision. The Board, on the other hand, publishes some of its decisions and expects that the data controllers are in compliance with such decisions. Such decisions, therefore, should be treated as principle decisions as well.

# Appeal and enforcement of the Board's decisions

As explained above, different types of sanctions may be imposed on the data controller and thus appellate mechanisms differ for different types of sanctions.

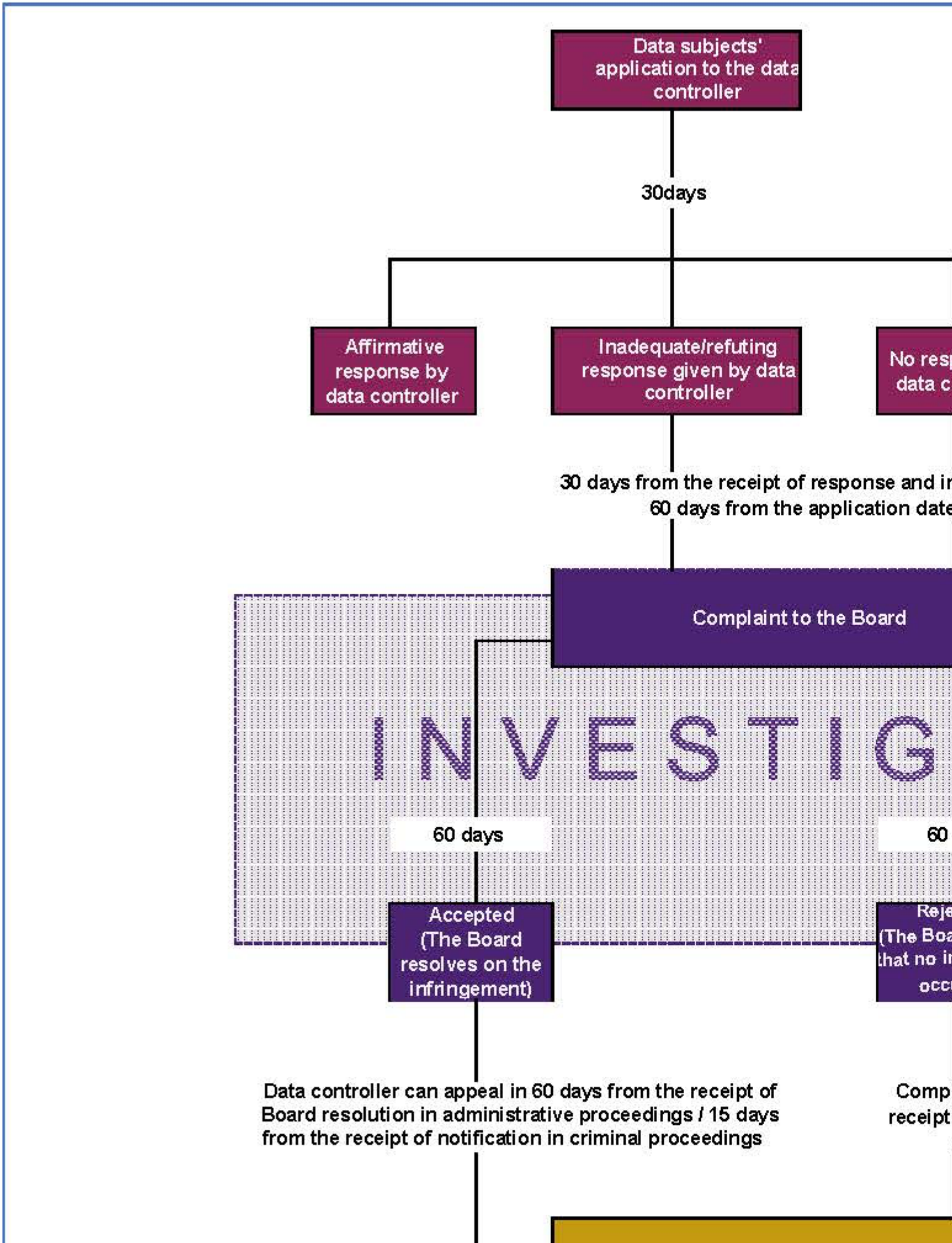
Assuming that only an administrative fine is imposed on the data controller, as the administrative fines are regulated by the Misdemeanors Law no matter under which regulation they are stipulated, the appellate mechanism under Article 27 of the Misdemeanors Law applies. According to this, a decision of the Board may be challenged by a data controller before the Criminal Court of Peace within 15 days as of the notification or pronunciation date of the decision. If no request of appeal is made within this period, the decision becomes final.

On the other hand, in case any other decisions are rendered by the Board on a data controller (for example any instructions given for remedying the infringement such as changing data processing operations, destructing data, rewriting information notices etc.), such action is deemed as an act of administration and will be subject to the appellate mechanism of administrative law. Data controllers may request an appeal within 60 days after the notification date before administrative courts as per Article 7 of the Administrative Jurisdiction Procedures Law No. 2577. In addition, the court's decision may be subject to appellate according to the general provisions of administrative law.

Board decisions are enforced in Turkey as per the administrative and enforcement laws of Turkey. However, as these are not court rulings, they do not benefit from general recognition and enforcement principles provided by international treaties. Therefore, for data controllers abroad, direct enforcement through recognition of the decision by the local court of the country of residence is not applicable. In this respect, these decisions may only be enforced

if there are bilateral agreements between Turkey and the country of residence which enable administrative sanctions to be recognised by the country of residence.

*Article first published on Data Guidance.*


Data subjects' application to the data controller
30days
Affirmative response by data controller
Inadequate/refuting response given by data controller
No resp
data c
30 days from the receipt of response and in
60 days from the application date
Complaint to the Board
INVESTIG
60 days
60
Accepted (The Board resolves on the infringement)
Reje
(The Boa
that no in
occ
Data controller can appeal in 60 days from the receipt of Board resolution in administrative proceedings / 15 days from the receipt of notification in criminal proceedings
Comp
receipt

## Related Practices

- Privacy and Data Protection

## Related Attorneys

- BURCU TUZCU ERS?N, LL.M.
- CEYLAN NEC?PO?LU, Ph.D, LL.M.