MOROĞLU ARSEVEN

The Decision of the Personal Data Protection Board regarding the Data Breach Notification Made by the Company Operating in the Health Sector

10 Feb 2021

The Personal Data Protection Board ("**Board**") has published its first decision where it does not impose any sanctions on the data controller who took all necessary technical and administrative measures after the data breach.

The data breach subject to the decision took place between 30 September 2020 and 5 October 2020. Taking advantage of the vulnerability in an application that is widespread throughout the world and is also used by the data controller, it has been detected by the data controller that a malicious software has been installed on the only server where the application is located.

As a result of an investigation carried out by the Board, it has been determined that;

1. Necessary trainings are given to the employees who are related to the violation, the trainings given by the data controller, the documents proving the participation status and the log records are submitted to the Board as an annex of the data breach notification form,

2. Prior to the data breach, all necessary technical measure were taken including;

- Network security and application security,
- Backing up personal data and ensuring the security of backups,
- Annual penetration tests,
- Use of data leakage prevention tools,
- Use of intrusion detection and prevention systems,

3. Prior to the data breach, all necessary administrative measures were taken,

4. After the data breach all necessary technical measure were taken including;

- Blocking external access to the location where the malicious software is hosted,
- Auditing the system with forensic software,
- Moving the backup system to a safe location,
- Continuing to confirm that the systems have not been seized, through the IOC information received from the expert firm from which the service is provided, and the rules provided by the incident response team, although it was not encountered in the first detections,
- Collecting necessary logs and records from end points identified as captured,

5. After the data breach all necessary administrative measure were taken.

Within this regard, the Board taken into consideration that;

- The breach was not caused by the lack of precaution of the data controller, but a common-used application; and the data controller cannot interfere in this situation,
- The data controller has noticed the violation in a short time,
- Personal data affected by the data breach can be easily obtained from company caches and public sources,
- The data controller stated that the persons affected by the breach will be notified within three business days,
- The low risk of negative impacts for the persons affected by the data breach,
- The data controller has taken reasonable technical and administrative measures,

and conclude that no further proceeding is required with respect to the data breach notification.

Please see this link for the summarized decision numbered 2020/787published on the Board's official website on 22 January 2021 (only available in Turkish).

Related Practices

- Privacy and Data Protection