

Personal Data Protection Board has published a Decision on Data Breach Notification of an Apparel Retailer

24 Dec 2021

The Personal Data Protection Board issued its decision dated 20 January 2020 and numbered 2020/50 regarding the personal data breach notification of an apparel firm, on its official website. The Board found it acceptable that the data controller residing abroad did not notify the breach within 72 hours in order to complete the necessary internal investigations after noticing the breach.

At the case in hand;

- The data breach occurred when 44 customers entered their personal data, such as e-mail address, date of birth, and password, into the system under the name of "required field" when creating a new account, and this data was leaked to third parties via an URL.
- This data has reached the internal systems of the data controller and some third-party vendors and providers, and the data controller has determined it in a regular audit. The data controller has notified the Personal Data Protection Authority ("**Authority**").
- Although it was confirmed that the data was deleted from the application analytics provider following the data breach notification submitted to the Authority, an investigation was carried out on the subject. Accordingly, it has been revealed that data was accidentally collected by other URLs and that this data was directed to the tag management system of the tag owner.
- Not only customers, but also subscribers, members and potential customers were adversely affected by the breach. It is possible that the name and surname data of these people may have been leaked. Eventually, the relevant persons were notified on 23 July 2019.
- The detection of data breaches that took place on 1 August 2018 and 21 October 2018 was made on 2 July 2019. Findings of the data breaches were completed in about a year due to the technical precaution deficiencies below:
 - Absence or inefficient use of company's log record/follow-up alarm systems,
 - Company's failure to provide necessary controls, and
 - The fact that personal data is transferred via URL is not revealed due to the lack of necessary tests during the design process of the company's website.
- For this reason, the Authority had decided to impose an administrative fine of TRY 50,000 on the data controller who did not take the necessary technical and administrative measures to ensure data security within the framework of article 12 of Personal Data Protection Law numbered 6698 ("**DP Law**"). In spite of the fact that the data controller was identified on 29 May 2019, no additional administrative fine was foreseen for the data breach notification to be made on 6 June 2019. After the date of detection of the violation by the data controller who residing abroad, the Authority has decided that this period is reasonable and that there is no action to be taken under the DP Law, as it is necessary to conduct an internal investigation to assess whether the relevant persons in Turkey are also affected.

You can access the details of the decision via this [link](#). (Only available in Turkish)

Related Practices

- [Privacy and Data Protection](#)
-

Related Attorneys

- [BURCU TUZCU ERSİN, LL.M.](#)
-