MOROĞLU ARSEVEN

# Personal Data Protection Board Publishes Ten Recent Decisions

*17 Aug 2021*

The following are summaries of ten recent decisions of the Personal Data Protection Board ("**Board**").

- **Decision No. 2020/216:** Regarding a cyber-attack in data controller's systems, the Board determined the following facts: (i) the data controller could not clearly determine which data in the system was accessed by the attackers and which personal data were affected; (ii) data of 65,993 people were kept in the system, and 1,784 of these persons had their old ID photocopies, (iii) in addition, 50,000 credit card information was stored in the system and (iv) high and medium-level vulnerabilities were detected in the web applications in the post-infiltration test. Considering these facts, the Board imposed a fine of TRY 450,000 on the data controller.
- **Decision No. 2021/407:** In the incident subject to the decision, the physician working in a hospital transferred the files of his patients from the archive out of the hospital through hospital staff by his instructions. The data breach was fully identified as a result of reviewing the CCTV footage 17 days after an employee was seen attempting to take the files out of the hospital. The Board determined that not all patient records could be retrieved after the incident, the data including the special category personal data were affected, the necessary training was not given to the employees, the breach was detected 17 days after the suspicion arose, the archive room was accessed by unauthorized persons, the established policies and procedures were not followed, and the breach was not reported to the Board on time. Considering these issues, the Board punished the data controller with an administrative fine of TRY 600,000.
- **Decision No. 2021/464:** The breach subject to the decision occurred when a hacker accessed the computer screen of an agency of the data controller insurance company. The Board determined that the data processor insurance agency was not adequately audited by the data controller insurance company, it is unknown whether any personal data was accessed, the agency employees were not adequately trained, outdated software was used and antivirus software was not used. As a result, the Board ruled a fine of TRY 60,000.
- **Decision No. 2020/466**: The breach subject to the decision occurred by wrong payrolls being sent to the e-mail addresses of the employees. The Board determined that corporate e-mail addresses were not provided to the employees, the payrolls are sent to the e-mail addresses at various e-mail servers notified to the employer by the employees, a risk assessment has not been conducted by the data controller, and there was not sufficient explanation regarding the issue in the privacy policy. As a result, the Board has ruled a fine of TRY 172,000.

- **Decision No. 2020/511:** The breach subject to the decision has occurred by making the identity and drug use information on a per-person basis accessible to 11 insured persons as a result of an error. Considering that the breach continued for more than 7 months, and the data controller noticed the breach after an insured person's notification; personal data including sensitive personal data were affected by the breach, vulnerability scanning had not been not performed, and the necessary security measures were not taken to prevent system failure, the Board decided to rule a fine of TRY 100,000.
- **Decision No. 2020/744:** The breach subject to the decision has occurred by a bank employee sharing the personal data of the bank with third parties. The Board determined that, (i) although the employees were trained, due to this breach, suspicions have arisen regarding the sufficiency of the content of the training, (ii), the e-mail containing personal data was not stopped by the leak prevention systems ("**DLP**"), and (iii) the data breach was not reported within the time limit. Considering these, the Board ruled a fine of TRY 275,000.
- **Decision No. 2021/154:** The breach subject to the decision has occurred when a former employee transferred the personal data of some customers that he had access to due to his duty, from his corporate e-mail address to a personal e-mail address with a G-mail extension. Taking into account the facts that the breach was noticed not by the data controller, but by the authorities at the next workplace of the employee, the DLP system did not prevent the leaking of the data in question, and adequate training was not provided,

the Board ruled a fine of TRY 150,000.

- **Decision No. 2021/187:** The breach subject to the decision occurred by sending the personal data of 681 data subjects to other customers as a result of a systematic error in the data processor from which the data controller received information system support service. The Board, taking into account the fact that the error in the application was not detected before the application was taken into operation, the breach was noticed after 2 years, and was not noticed by the data controller on its own, ruled a fine of TRY 125,000.
- **Decision No. 2021/190:** The breach subject to the decision has occurred by a branch employee monitoring the identity data of customers, taking their pictures with his personal mobile phone and sharing it with a third party. Considering that the training provided was not sufficient to raise awareness of the employees, team leaders were able to view customer data whenever and as often as they wanted, there was no inquiry quota application, and there was no warning system, the Board ruled a fine of TRY 100,000.
- **Decision No. 2021/311:** The breach subject to the decision has occurred as a result of a change made in the website of the data controller. The members of the website accessed the member information of someone else when they logged into the website. Considering the fact that it could not be determined how many people had access to the data, the changes made on the site were implemented in the peak time zone and not the time with the lowest access to the site, and encryption and masking measures were not taken, the Board decided to impose a fine of TRY 200,000.

## Related Practices

- Privacy and Data Protection

## Related Attorneys

- CEYLAN NEC?PO?LU, Ph.D, LL.M.