11 Recent Decisions of the Personal Data Protection Board

3 Sep 2021

The following are summaries of 11 recent Personal Data Protection Board (the "**Board**") decisions published on 2 August 2021:

- **Decision No. 2019/170:** a fine of TRY 50,000 was levied on data controller. Board findings: (i) data breaches were detected nearly one year after occurrence due to lack of internal controls, including transaction logs and breach notification systems, or ineffective implementation thereof, (ii) inclusion of personal data in third party URLs indicates either insufficient testing during webpage design or no testing at all.
- **Decision No. 2020/113:** a fine of TRY 200,000 was levied on data controller. Board findings: (i) prior to the data breach, data controller's systems were accessible without restriction via shared public WiFi points outside of data controller's control (e.g., coffeehouses) (ii) data breach tests were performed only post-breach (iii) vulnerabilities that could allow unauthorized access to critical information maintained by data controller were revealed (iv) mobile app lacked an SSL Certificate and unencrypted app traffic was subject to eavesdropping, (v) data security protocols and breach response plans were established only post-breach, (vi) pre-breach, staff were not trained in breach prevention and breach management, and (vii) data controller became aware of the breach only after notification by attacker.
- **Decision No. 2020/201:** a fine of TRY 75,000 was levied on data controller. Board findings: (i) data controller sent 905 misaddressed e-notifications containing customer personal data, (ii) data controller lacked appropriate internal controls, the errors lead to the breach should have been detected during the testing phase and the changes should have been corrected before they were published.
- **Decision No. 2020/357**: a fine of TRY 90,000 was levied on data controller. Board findings: (i)Personal Data Protection Law numbered 6698 ("**DP Law**") violation resulted from subcontractor sending from assigned corporate email address to personal email address a customer list showing names and surnames, contact info., and license plate data of 91 customers, (ii) appropriate internal controls could have prevented the violation, (iii) data controller provided data protection training only to select employees.
- **Decision No. 2020/530:** a fine of TRY 200,000 levied on data controller. Board findings: (i) the employee who caused the breach carried out 10,529 Credit Bureau of Turkey inquiries for 1,052 people between 1 January 2019 and 5 December 2019, without any reasonable explanation (ii) the employee is suspected to leak customer information outside the bank, (iii) pre-breach data controller did not limit employee's Credit Bureau inquiries (iv) data breaches were detected upon a notification nearly one year after occurrence due to lack of internal controls, and this implied that adequate inspection and surveillance were not carried out.
- **Decision No. 2020/567:** a fine of TRY 75,000 was levied on data controller. Board findings: (i) two-factor authentication protocol was not implemented prior to breach, (ii) pre-breach, customers not required to create a strong password when opening an account, and (iii) inadequate web application firewall kicked in only after significant unauthorized personal data accessed.
- **Decision No. 2020/715:** a fine of TRY 165,000 levied on data controller. Board findings: (i) unauthorized access to data subject accounts containing personal data was a data breach, (ii) no pre-breach limit on failed login attempts from a single IP address, (iii) pre-breach users were not required to change passwords at prescribed intervals, (iv) log of successful logins following repeated failed attempts from same IP address were not routinely reviewed pre-breach.
- **Decision No. 2020/816:** Fine was not levied on the technology company as a data controller. Board findings: (i) personal data of a single individual was emailed in violation of the DP Law, (ii) affected individual was timely notified by telephone, (iii) the nature of the personal data at issue renders a negative impact on data subject unlikely, (iv) the offending email is deleted, and (v) data controller timely intervened to prevent successive violations.
- **Decision No. 2020/935:** fine was not levied on the insurance company as a data controller. Board findings: (i) personal data of a single individual was emailed in violation of the DP Law, (ii) affected individual was timely notified by telephone, (iii) the nature of the personal data at issue renders a negative impact on data subject unlikely, (iv) the offending email is deleted, and (v) data controller timely intervened to prevent

successive violations.

- **Decision No. 2020/957:** fine was not levied on data controller. Board findings: (i) individual employee payroll data including personal data was emailed to various employees in violation of the DP Law, (ii) violation occurred during a transition to a higher security server, (iii) violation was detected within 13 minutes and remediated within 2 hours, (iv) the nature of the personal data at issue renders a negative impact on data subject unlikely, (v) the offending emails are deleted and affected individuals were timely notified, (vi) necessary data protection measures have since been implemented.
- **Decisions No. 2021/511-512-513:** Petitioner contended that attorneys accessed certain personal debt information and other personal data from execution offices. The Board found no DP Law violation because Attorney Law numbered 1136 law explicitly grants attorneys the right to access pending court and execution office case files.

Related Practices

- Privacy and Data Protection

Related Attorneys

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