MOROĞLU ARSEVEN

Nine Recent Decisions of the Personal Data Protection Board

3 Sep 2021

The following are summaries of nine recent Personal Data Protection Board (the "**Board**") decisions published on 9 August 2021:

- **Decision No. 2020/50:** 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, and (ii) inclusion of personal data in third party URLs indicates either insufficient testing during webpage design or no testing at all
- **Decision No. 2020/345:** a fine of TRY 130,000 was levied on data controller. Board findings: (i) the fact that without authorization and after termination a former employee could and did copy and upload to GitHub data controller's e-file containing certain source code and other data files demonstrated systemic vulnerability and was a violation of the Personal Data Protection Law numbered 6698 (the "**DP Law**"), (ii) the violation was first identified nearly two years after it occurred, (iii) the facts demonstrate a lack of adequate internal controls, including transaction logs and breach notification systems, or ineffective implementation thereof, and (iv) the violation was not timely reported.
- **Decision No. 2020/359:** a fine of TRY 450,000 was levied on the data controller. Board findings: (i) DP Law violation continued for nearly one year, in between annual Credit Bureau inquiry audits, (ii) appropriate data protection measures were such as authorization limitation in user based log records, closing screens to unnecessary roles, popping a warning text regarding the protection of personal data, implemented only post-breach, (iii) inadequate employee training in data protection, (iv) violation was not timely reported.
- **Decision No. 2020/421**: a fine of TRY 210,000 was levied on data controller. Board findings: (i) system was breached by hackers after login attempts from some 14,000 IP addresses of which 2,092 were successful (ii) the anomalous traffic went unnoticed by data controller which became aware of the breach only when notified by the hacker, (iii) failure to identify the unusual traffic, except those 2,092 hacked accounts, demonstrated a lack of adequate internal controls, including logs and breach identification and notification systems, or ineffective implementation thereof.
- **Decision No. 2020/463:** a fine of TRY 125,000 was levied on data controller. Board findings: (i) certain critical data of multinational data controller were deleted by hackers, (ii) only when employees reported system lockouts at their terminals did data controller uncover the breach (iii) facts demonstrate a lack of adequate internal controls, including logs and breach identification and notification systems, or ineffective implementation thereof.
- **Decision No. 2020/465:** a fine of TRY 75,000 levied on data controller. Board findings: (i) the breach was discovered nearly five months after it occurred, (ii) password spraying attack on data controller demonstrate the end users' lack of awareness of password security, (iii) over 6 TB of data were stolen, due to the overmuch amount of data stored in the drive.
- **Decision No. 2020/532:** a fine of TRY 30,000 levied on data controller. Board findings: (i) system error permitting post-launch app data breach caused by obsolete software, (ii) breach went undetected for five days, (iii) since data controller handled sensitive insurance transactions the system error should have been identified and remediated pre-launch.
- **Decision No. 2020/763:** fine was not levied on data controller. Board findings: (i) 43 data subject email addresses, names and surnames were shared electronically with 400 other individuals in violation of the DP Law, (ii) affected data subjects and the Board were timely notified, (iii) the nature of the personal data at issue renders a negative impact on data subjects unlikely, (iv) data controller requested of all 400 recipients that they delete the offending email.
- **Decision No. 2020/934:** fine was not levied on data controller. Board findings: (i) only two users were affected by the breach (ii) the file could have been accessed by only eight other users, (iii) each of these eight other users confirmed that they would not use or share same, (iv) the nature of the personal data at issue renders a negative impact on data subjects unlikely, (v) the platform now masks user passwords, (vi)

data controller deleted the breached password files, notified all platform users of the breach and required all to change passwords.

Related Practices

- Privacy and Data Protection

Related Attorneys

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