MOROĞLU ARSEVEN

The Personal Data Protection Board Published a Public Announcement on The Technical and Administrative Measures Recommended by Data Controllers regarding User Security

15 Apr 2022

After the publication of the guide on technical measures, the Personal Data Protection Board ("**Board**") also published a public announcement on which technical measures should be taken by data controllers and their reasons.

The most important provisions of the announcement dated 15 February 2022, are as follows:

- The data breach notifications recently submitted to the Board have been evaluated within the scope of the obligation of data controllers to take all necessary technical and administrative measures to ensure the appropriate level of data security in accordance with article 12 of Personal Data Protection Law numbered 6698.
- The user account information (username and password) used to log into the websites of data controllers operating in sectors such as finance, e-commerce, social media, and gaming are publicly available on some websites.
- As a result of obtaining user account information by third parties, the following issues have been determined:
    - Active access to the websites of data controllers without the knowledge of the users,
    - Access to end users' computers without their consent by using system and security vulnerabilities of data controllers and the personal data obtained are offered for sale for an economic value,
    - This data is archived and remarketed as data sets by malicious third parties.
- The Board has stated that the risk on the data subjects can be minimized by preventing possible data breaches with the technical and administrative measures to be taken by the data controllers and data processors of the institution within the scope of data responsibility.
- The Board recommended that data controllers take the necessary technical and administrative measures by making risk assessments in order to prevent common data breaches and to reduce the possibility of harming the data subject in the event of a data breach.

The measures recommended by the Board are listed below:

- Establishing two-factor authentication systems and presenting them to their users as an alternative security measure starting from the membership application stage.

- In case of logging in on different devices other than devices that provide frequent access to users' accounts, ensuring that the login information is forwarded to the contact addresses of the relevant persons via e-mail/SMS or other similar methods.
- Protecting applications with HTTPS (Hypertext Transfer Protocol Secure - Hypertext Transfer Secure Protocol) or in a way that provides the same level of security.
- Using secure and up-to-date hash (hashing) algorithms to protect user passwords against cyber-attack methods.
- Limiting the number of unsuccessful login attempts from the IP (Internet Protocol Address) address.
- Ensuring that the relevant persons can view their information about at least the last five successful and unsuccessful login attempts.
- Reminding the relevant persons that the same password should not be used on more than one platform.
- Creating a password policy by data controllers and ensuring that users' passwords are changed periodically or reminding the relevant persons about this issue.
- Preventing newly created passwords from being the same as old passwords (at least the last three passwords), using technologies such as security codes (such as CAPTCHA, four processes) that distinguish computer and human behaviors when logging into user accounts, limiting the IP addresses that are allowed to be accessed.
- Ensuring that the length of the passwords entered into the systems of data controllers is at least ten characters, and strong passwords are created for the use of upper- and lower-case letters, numbers and special characters together.
- If third-party software or services are used to access the systems of data controllers, regularly performing security updates of these software and services and making necessary checks.

The full decision is available at this link. (Only available in Turkish).

Related Practices

- Privacy and Data Protection

Related Attorneys

- BURCU TUZCU ERSİN, LL.M.
- CEYLAN NECİPOĞLU, Ph.D, LL.M.