MOROĞLU ARSEVEN

Turkey’s Data Protection Board Announces Rules for Processing Special Categories of Personal Data

22 Mar 2018

Turkey's Personal Data Protection Board ("**Board"**) has announced rules for processing special categories of personal data. Notably, data controllers must prepare a separate policy and procedure for protecting special categories of personal data. The Board also emphasized the importance of the measures which had previously been determined in the Personal Data Security Guide.

Turkish legislation deems the following personal data to fall into a special category, subject to increased rules and requirements: race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, biometric and genetic data. Legislation states that persons processing special categories of personal data must take adequate measures, as announced by the Board (Article 6/4 of Personal Data Protection Law number 6698).

Accordingly, the Board announced that data controllers processing special categories of personal data must:

- Prepare a separate policy and procedure for processing special categories of personal data.
- Take certain measures for employees involved in processing such data, such as:
    - Organize the required trainings.
    - Arrange and sign confidentiality agreements.
    - Determine access rights and regularly make authority checks.
    - Immediately remove authority from employees which change duties or leave the company.
    - Retrieve any data inventory assigned to the employee.
- Take certain measures when processing such data in an electronic environment, such as:
    - Keep the data by using cryptographic methods and keep cryptographic authentication keys in secure and different environments.
    - Keep data processing logs in a secure manner.
    - Constantly undertake security updates for the data processing environments.
    - If data is accessed through software, take certain specified measures regarding use of the software.
    - Use at least a two-step verification for remote access to data.
- Take certain measures while processing such data in a physical environment, such as:
    - Take adequate security measures depending on the nature of the physical environment (electrical leakage, fire, flood, burglary, etc.)
    - Secure the physical environment and prevent any unauthorized entry.
- Take certain measures for transferring of such data, such as:
    - Use corporate e-mail and registered e-mail systems as well as encryption for transfers via e-mail.

- Use cryptographic encryption and keep the cryptographic keys in different environments for transfers via USBs, CD or DVDs etc.
- Use VPN or sFTP methods for transfers between different servers in different physical environments.
- Take necessary measures to prevent risks such as loss or burglary and identify the document as "confidential", if data is transferred on paper.

The Board's Decision number 2018/10, dated 31 January 2018 was published in Official Gazette number 30353 on 7 March 2018. The full text can be found at this link (only available in Turkish).

Related Practices

- Privacy and Data Protection
- Information Technologies

Related Attorneys

- BURCU TUZCU ERS?N, LL.M.