

The decision of the Personal Data Protection Board dated 31/01/2018 numbered 2018/10 concerning "Adequate Measures That Must be Taken About Special Categories of Personal Data by the Data Controllers "

Decision Date : 31/01/2018

Decision Number : 2018/10

Summary of the Subject : Discussion on "Adequate Measures That Must be Taken About Special Categories of Personal Data by the Data Controllers"

It has been unanimously resolved to agree on the "Adequate Measures That Must be Taken About Special Categories of Personal Data by the Data Controllers" drafted based on paragraph (4) of article 6 and sub-paragraph (ç) of the first paragraph of article 22 of the Law as follows and to publish such decision in the Official Gazette.

Adequate Measures That Must be Taken About Special Categories of Personal Data by the Data Controllers

Paragraph (4) of article 6 of Law numbered 6698 concerning Personal Data Protection (Law) provides that *"It is additionally required to take the adequate measures designated by the Board when special categories of personal data are processed."*

In this regard, the adequate measures that must be taken by the data controllers that process special category of personal data as per sub-paragraphs (ç) and (e) of the first paragraph of article 22 of the Law are determined by the Personal Data Protection Board as follows:

- 1- To determine a separate policy and procedures for the security of the special category of personal data that are systematic, the rules of which are precisely provided, that can be managed and sustainable,
- 2- With respect to the personnel who are involved in the process of processing special category of personal data;
 - a) to give regular trainings on the Law and related legislation as well as the security of special category of personal data,
 - b) to enter into confidentiality agreements,
 - c) to specify the scope of the authority and terms of service of the users who have authority to access to data precisely,

ç) to control authorities periodically,

d) to cancel such authorities of the personnel whose service is changed or employment contract is terminated promptly. In this respect, to receive back the inventory that is assigned to him/her by the data controller,

3- In case the platform where the special category of personal data are processed, stored and/or accessed are electronic;

a) to store the data by using cryptographic methods,

b) to keep the cryptographic keys in secured and different platforms,

c) to log securely the transaction records of all actions realized on the data,

ç) to follow constantly the security updates for the platforms where the data are found, to perform necessary security tests regularly or have them performed, to record the test results,

d) to authorize users for the software where the data are accessed through a software, to perform regularly security tests on such software or have them performed, to record the test results,

e) to set at least two-step identity verification system where remote access to data is needed,

4- In case the platform where the special category of personal data are processed, stored and/or accessed are physical;

a) to ensure provision of adequate security measures (against situations such as leakage of electricity, fire, flood, theft, etc.) taking into consideration of the type of the environment where special category of personal data are found,

b) to restrain unauthorized entry and exit by providing physical security of the environment,

5- In case the special category of personal data shall be transferred;

a) to transfer data by an encrypted way and through corporate e-mail address or using Secured Electronic Mail (SEM), where data must be sent via email,

b) to encode by an encrypted way and keep the cryptographic key in a different environment, where transmission must be made by environments such as memory stick, CD or DVD,

c) to transfer data by setting up VPN or through sFTP method between servers where the transmission is between servers at different physical environments,

ç) to take necessary measures against the risks such as stealing or loosing of documents or having seen them by unauthorized persons and to transfer the documents in a form of “classified document”, where transmission must be made by hardcopy environments.

6- In addition to the above measures, technical and administrative measures must also be taken into consideration to ensure the adequate security level that is envisaged in the Personal Data Security Guide published on the website of the Personal Data Protection Board.