DOKU AESTHETIC AND HEALTH SERVICES

PROCESSING OF SPECIAL CATEGORY PERSONAL DATA POLICY AND PROCEDURE

Article 6 (4) of the Personal Data Protection Law No. 6698 (the Law) stipulates, "In the processing of special category personal data, it is required to take adequate measures determined by the Board."

In this context, in accordance with subparagraphs (ç) and (e) of paragraph (1) of Article 22 of the Law, the adequate measures to be taken by data controllers processing special category personal data have been determined by the Personal Data Protection Board.

As a Data Controller, in the processing of special category personal data, it is necessary to determine a separate policy and procedure that is systematic, has clear rules, and is manageable and sustainable for the security of special category personal data.

1. Special Category Personal Data can only be processed with the explicit consent of the Data Subject or, in cases where the processing of Special Category Personal Data other than sexual life and personal health data is explicitly required by law.
2. Personal Data concerning health and sexual life can be processed without obtaining explicit consent only by persons under the obligation of confidentiality (e.g., company doctors) or authorized institutions and organizations for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, and planning and management of health services and financing.
3. When processing Special Category Personal Data, the measures determined by the Board are taken.
4. The Company will provide regular training on the Personal Data Protection Regulations and the security of Special Category Personal Data for employees involved in the processing of Special Category Personal Data.
5. Confidentiality agreements will be made.
6. The Company will clearly define the scope and duration of the authorization for users with access authorization to Special Category Personal Data.
7. Periodic authorization checks will be performed.
8. The Company will immediately revoke the permissions in this area for employees who have changed positions or left the job and will immediately retrieve the inventory allocated to the relevant employee.
9. In case of transferring Special Category Personal Data to electronic environments, the Company, with respect to electronic environments where Special Category Personal Data is processed, stored, and/or accessed, will:

9.1. Store Special Category Personal Data using cryptographic methods.

9.2. Keep cryptographic keys securely and in separate environments.

9.3. Securely log all transaction records of operations carried out on Special Category Personal Data.

9.4. Continuously monitor security updates for the environments containing Special Category Personal Data, conduct necessary security tests regularly or have them conducted, and record test results.

9.5. If Special Category Personal Data is accessed through a software tool, the Company will carry out user authorizations for this software, conduct security tests regularly or have them conducted, and record test results.

9.6. In case of remote access to Special Category Personal Data, provide at least a two-step authentication system.

10. In case of processing Special Category Personal Data in a physical environment, the Company, with respect to the physical environments where the data is processed, stored, and/or accessed, will:

10.1. Ensure that adequate security measures (against electrical leakage, fire, flood, theft, etc.) are in place according to the nature of the environment containing Special Category Personal Data.

10.2. Ensure the physical security of these environments by preventing unauthorized entries and exits.

11. In case of transferring Special Category Personal Data, the Data Controller will:

11.1. Use encrypted corporate email addresses or Registered Electronic Mail ("REM") accounts if it is necessary to transfer Special Category Personal Data via email.

11.2. Encrypt the data using cryptographic methods and store cryptographic keys in a separate environment if it is necessary to transfer Special Category Personal Data via portable memory, CD, DVD, or similar media.

11.3. Set up a VPN between servers or use the SFTP method for transferring Special Category Personal Data if it is necessary to transfer the data between servers in different physical environments.

11.4. Take necessary precautions against risks such as theft, loss, or unauthorized access to the document and send the document in a "classified documents" format if it is necessary to transfer Special Category Personal Data via paper.

12. In addition to the above regulations, the Company will act in accordance with the Personal Data Protection Board's published regulations, primarily the Personal Data Security Guide, to ensure the security of Personal Data, including Special Category Personal Data.

13. In every situation that requires the processing of Special Category Personal Data, the relevant employee shall inform the [Data Controller Representative and/or Committee].

14. If it is unclear whether a piece of data is Special Category Personal Data, the relevant department will seek the opinion of the [Data Controller Representative and/or Committee].