

Personal Data Processing, Protection, and Destruction Policy (Translation)

Purpose and Scope

This policy establishes the procedures and principles related to the processing, storage, and destruction of personal data in our clinic. Our clinic prioritizes the lawful processing of personal data belonging to employees, candidates, service providers, patients, and other third parties, ensuring the rights of data subjects as stipulated by the Turkish Constitution, international agreements, the Law on Personal Data Protection (No. 6698), and other relevant legislation.

Definitions

- Consent: Voluntary, informed consent regarding a specific issue.
- Anonymization: Rendering personal data unidentifiable with any individual, even if matched with other data.
- Data Subject: Individual whose personal data is processed.
- Personal Data: Any information relating to an identified or identifiable individual.
- Sensitive Personal Data: Data regarding race, ethnicity, political opinions, religious beliefs, health, sexual life, and other private matters.
- Data Processor: Entity processing data on behalf of the data controller.
- Data Controller: Entity responsible for data processing decisions and management.

Data Processing Principles

Personal data processing is carried out in accordance with the principles set forth in the Law, including:

- Lawfulness and honesty.
- Accuracy and up-to-date processing.
- Processing for specific, explicit, and legitimate purposes.
- Data minimization.
- Storage for no longer than necessary.

Data Processing Exceptions

Except in specific cases, personal data is processed with consent. Exceptions include situations where:

- Data processing is mandated by law.
- Data processing is essential to protect someone's life or bodily integrity.
- Processing is necessary to establish or execute a contract.
- Data controller has legal obligations.
- Data subject has made the information public.
- Processing is needed to establish, use, or protect a right.
- Data processing is mandatory due to data controller's legitimate interests.

Sensitive Personal Data

Sensitive personal data is processed only with explicit consent unless legally mandated otherwise.

Storage and Destruction

Personal data is stored per legal requirements and securely deleted, destroyed, or anonymized at the end of the retention period. Data storage complies with laws such as the Turkish Obligations Law and the Health Insurance Law. The clinic conducts periodic deletions every June and December.

Technical and Administrative Measures

Technical measures include strong passwords, regular backups, access limitations, and encrypted transmission for sensitive data. Administrative measures involve regular staff training, confidentiality agreements, and data security policy enforcement.

Destruction Techniques

At the end of the retention period, data is securely erased and rendered inaccessible and irretrievable in both electronic and physical formats.

Retention and Disposal Times

Retention and disposal schedules are outlined in the data inventory table and can be accessed on 'verbis.kvkk.gov.tr.'

Periodic Disposal Period

Periodic disposal is conducted bi-annually in June and December, per the regulations.

Policy Publication and Update Period

The policy is published in both hard copy and electronic formats and reviewed for updates as needed. Any changes are communicated on the clinic's website.

Policy Enforcement and Termination

The policy takes effect once published on the clinic's website. If revoked, it will be archived with signatures and stored for a minimum of five years.