



DOĞUŞ UNIVERSITY

Policy on Privacy of Personal Data and Its Destruction

1. Purpose of the Policy

The purpose of our personal data retention and destruction policy is to reveal the philosophy, purpose and action plan so as to determine the maximum time required for the purpose of processing the personal data as data responsible, while performing the transactions of deleting, destroying and anonymizing the data. In this context, our aim is to inform our students, graduates, administrative and academic staff, visitors and the institutions we cooperate with, and all third parties who are in contact with Doğuş University (DOU) in terms of the processing and rights of their data; and executing transactions ensuring the transparency in this regard while respecting the private life.

2. Support of this Policy

Our Policy was generated as per the Privacy Act dated 7.4.2016 numbered 6698 (Privacy Act numbered 6698.) and Directive on Deletion, Destruction and Anonymizing the Personal Data having taken effect after being published on the Official Gazette dated 28.10.2017 and numbered 30224, articles 5 and 6.

3. Scope of the Policy

Our Policy encompasses our students, graduates, administrative and academic personnel, our visitors and institutions with whom we are in collaboration and all natural and legal persons who are in legal relations with DOU and all their private and non-private data set forth under Privacy Act numbered 6698.

The Policy encompassed as set forth under Privacy Act numbered 6698, provided that it is part of a data registry system completely or partially where they are processed with non-automatic methods. Unless otherwise indicated in the policy, personal information and special private information shall jointly be referred to as "Personal Data".

4. Definitions

Interested person: Natural person whose data is being processed,

Personal Data: All kinds of data of natural persons who can be identified,

Special personal data: Biometric and genetic data and the data of individuals related to race, ethnic origin, political thought, philosophical belief, religion, sect or other beliefs, dress and attire, association, foundation or trade union membership, health, sexual life, criminal conviction and security measures,

Explicit Consent: Consent disclosed relating to certain matters, based on informing and with free will,

Data Supervisor: The natural or legal person (Doğuş University) who is responsible for setting up and managing the data recording system, determining the purposes and means of processing the personal data,

Processing the personal data: Any kind of operation on data executed relating to personal data provided that they are part of a data registry system such as obtaining or recording, storing, retaining, altering, re-arranging, disclosing, transferring, taking over, making available, making, classification or preventing the use of personal data in whole or in part automatically or as part of any data logging system,

Destruction: Deleting the personal data, their destruction or anonymizing,

Table for retaining and destroying personal data: The table which shows the durations for keeping the personal information by the University,

Personal Data processing inventory: Processing of personal data which are carried out by data responsible according to business processes; personal data, data category, transferred group of recipients and group of data to the group of people they created and personal data, the maximum amount of time required for the purposes for which they are processed, personal data prescribed to foreign countries and the measures taken in relation to data security.

Deleting personal information: Rendering the personal information inaccessible or un-obtainable by the interested users in any way whatsoever,

Destruction of personal data: Rendering the personal information inaccessible, un-recoverable or un-obtainable by the interested users in any way whatsoever,

Anonymizing: Even if the personal data are matched with other data, rendering them not identifiable or affiliated with a natural person,

Periodical destruction: If the personal data processing conditions set forth under law are completely eliminated, the deleting, destroying or anonymizing transactions set forth under personal data retaining and destruction policy and to be performed ex-officio with certain intervals,

Data registry (retention) system: The registry system whereby personal data are structured based on certain criterions and processed,

Board: Personal Data Protection Board

Committee: shall refer to Personal Data Protecting Committee.

5. General Principles on which the Policy is based

In processing the personal data by the data supervisor Doğuş University, the following principles shall be abided by.

5.1. Personal information may only be processed only as per the principles and methods set forth under Privacy Act numbered 6698.

5.2. The following principles shall be observed in processing the personal data:

- a)** Being legal and within rules of integrity.
- b)** Being accurate and up-to-date as required.
- c)** Being processed for certain, clear and legitimate purposes.
- d)** Being connected, limited and proportionate to the purposes of their processing.
- e)** Being retained for the periods envisaged under the relevant legislations or for their processing purposes.

6. Recording Environments whereby the Policy is regulated

Provided that it is a part of a data registry process which is fully or partially automated, all environments where personal data processed by non-automatic ways are kept shall be deemed as registry environments.

7. Personal Data Protecting Committee's duties and authorities

7.1. Personal Data Protecting Committee shall be responsible from announcing this Policy to the related business units and following up its requirements and fulfilling them by the concerned units of DOU.

7.2. If the Personal Data Protecting Committee is to cause the concerned business units for the Directive changes on protecting the personal data, regulating transactions of Personal Data Protecting Committee and their decisions, court orders or changes in processes, implementation and the system, the required notifications and announcements shall be made required for business process updates.

7.3. Personal Data Protecting Committee shall determine the processes for inspecting, assessing, following up and concluding on the processes under Privacy Act numbered 6698 and secondary regulations, the decrees of the Board and regulations, court orders and decisions of other authorized bodies and/or requests, assessing them, following them up and concluding them and notifies them to the concerned units.

8. The Actions to be taken in cases where the Processing conditions for the personal data vanish

8.1. In cases of objective element for processing the personal data being vanished, the explicit consent being retracted or the conditions for processing the personal data stipulated under articles 6 and 6 of Privacy Act numbered 6698 or in cases where none of the exemptions set forth in the relevant articles are going to be implemented, the personal data for which the processing conditions vanished, shall be deleted, destroyed or anonymized by the relevant business unit taking into consideration the business requirements, within the scope of articles 7 and 10 of the Directive, also clarifying the grounds for the method implemented. However if there is a finalized court order, it is statutory that the method of destruction decided by the court decree is to be implemented.

8.2. The users processing or retaining the personal data and the data holder DOU units shall review whether the conditions of processing have vanished or not within periods of six months at the latest to be reviewed in the data registry environments they use. Upon the application by the personal data holder or the notification by the Board or the court, the relevant user and units shall carry out this review in their data registry environments they use without regard for the periodical inspection term.

8.3. As a result of the periodical inspections or when it is determined that data processing conditions have been eliminated at any moment, the concerned user or data holder shall decide the relevant personal data to be deleted from the recording environment it has as per this policy, its destruction or anonymizing it. In cases of doubt, the transaction shall be executed after receiving the required opinion from the data holder/owner business unit. When the decision is to be taken relating to the destruction of personal data subject to multiple owners/stakeholders, the opinion of the Personal Data Protection Committee shall be taken and the person in question shall decide regarding the personal data in question including keeping or deleting the data as per this policy, its destruction or its being anonymized.

8.4. All transactions executed relating to the deletion of personal data, their destruction or anonymizing shall be recorded and the records in question shall be retained for a term of three years at least excluding the other legal obligations.

8.5. As per articles 4 and 7 of the Directive, the methods implemented relating to the deletion of personal data, their destruction and anonymizing them shall be clarified on the Data Destruction Procedure which is to be published after this policy takes effect.

8.6. It is mandatory that in deleting, destroying or anonymizing of the personal data, the general principles under article 4 of Privacy Act numbered 6698 and the technical and administrative precautions to be adopted as per article 12 of Privacy Act, provisions of relevant

legislation, Board resolutions and preserving and destroying the personal data policy shall be observed and abided by.

8.7. The natural person who possesses the personal data may apply to DOU, based on article 13 of Privacy Act numbered 6698 and request its personal data to be deleted, to be destroyed or when there is a request for anonymizing it. It shall inspect whether the conditions for processing the personal data were eliminated or not by the relevant data holder business unit. If all processing conditions were eliminated; it shall delete the personal data subject to the request, destroy them anonymizing them. In this case, in such a way that its details shall be determined by the Data Destruction Procedure; the request shall be concluded within thirty days at the latest following the date of application and the applicant shall be informed by the interested authority. If the entire conditions for processing personal data have been eliminated and the personal data which are subject to the request have been transferred to third parties, then the relevant data owner business unit shall notify this to the third party to whom transfer is being made immediately and ensures that the required action is taken within the scope of the Directive relating to the third party.

8.8. In cases where the circumstances for processing the personal data do not disappear totally, the requests of the holders of personal data for deleting or destroying the personal data may be rejected by DOU based on 3rd clause of article 13 of Privacy Act numbered 6698. The rejection reply shall be notified to the interested person within 30 days at the latest in written form or via electronic environment.

8.9. Requests for the deletion or destruction of personal data shall be assessed only if the person concerned has been identified. In requests to be made outside the channels in question, the persons concerned shall be directed to the channels whereby identification or identity verification can be made.

9. Enforcing the Policy, Cases of violations and sanctions

9.1. This Policy shall enter into force upon notice to all employees and shall be binding for all business units, consultants, external service suppliers and anyone who process personal data at DOU.

9.2. The follow-up of whether the employees of DOU meet the requirements of the Policy will be the responsibility of their respective supervisors. When a violation of the policy is determined, a supervisor of the relevant employee shall immediately inform the subject. In case of a violation of significant size, the Supervisor shall inform the Committee on Protection of Personal Data without any delay.

9.3. The necessary administrative action shall be taken after the evaluation by the Personnel Department about the employee who violates the policy.

9.4. For the fulfilment of policy requirements; All necessary safety measures, including the ISO standard and measures required by Higher Education Council are taken

10. Persons and their Responsibilities authorized for the Storing and Disposal of Personal Data

All employees, consultants, external service providers and other persons who store and process personal data at DOU are responsible for fulfilling these requirements in the fulfilment of the requirements for the destruction of data specified in the Regulation and Article 6698 of Privacy Act within DOU.

Each business unit is responsible for preserving and protecting the data generated in its business processes; but if the data produced is only in the information systems except for the control and authorization of the business unit, the data will be kept by the units responsible for the information systems.

The periodic destruction that will affect the business processes and cause the data integrity to be impaired, data loss and legal regulations will be made by the related information systems departments taking into account the type of personal data, the systems considering the business owner units.

11. Retaining and Elimination Periods of Personal Data

You may find below the Table for Storing and Disposing Periods of Personal Data. In case of periodic destruction or on-demand disposal, such storage and disposal times shall be taken into consideration. The business units will be updated on the basis of the evaluation of the Committee for the Protection of Personal Data, if in doubt

12. Periodical Periods of Destruction

Periodical periods of elimination of the Personal Data shall be determined by the relevant business units who hold the data. Such periods shall not exceed 6 (six) months.

13. Enforceability

13.1. The Policy shall take effect on the date of its being published.

13.2. Announcing the Policy within DOU in general and doing the required updates is the responsibility of Committee for Protecting Personal Data.

Table for Storing and Disposing Periods of Personal Data

Unless there is any finalized court decision or precautionary decision, otherwise, the matters set forth under article 6 of the policy shall be considered in terms of storing/keeping the data for the periods set forth on the following table and they shall be terminated at the end of the term.

As per article 146 of Turkish Code of Obligations numbered 6098 which regulates the general lawsuit time-lapse duration	10 years
As per other relevant legislation	As long as the term set forth under the relevant legislation

If the personal data in question is subject to a crime which requires penalty under Turkish Penal Code or other regulations requiring penalty or being related with a crime, as per articles 66 and 68 of Turkish Penal Code numbered 5237	As long as the durations set forth under lapse of time for lawsuits and lapse of time and Judicial Registry Law numbered 5352.
--	--