Central Finance and Contract Unit (CFCU)

Policy on Storage and Disposal of Personal Data

1. Objective

This Policy, the Policy on Storage and Disposal of Personal Data, is prepared by the CFCU in order to determine the procedures and principles regarding the work and transactions related to the storage and disposal activities carried out by the Central Finance and Contracts Unit (UNIT) as the Data Controller, by taking into account the provisions stated in 'the Policy on Processing and Protection of Personal Data of the CFCU' and 'the Policy on Adequate Measures to be Taken by the CFCU as the Data Controller in the Processing of Sensitive Personal Data'.

In line with its mission, vision and basic principles, the CFCU gives priority to the processing of personal data belonging to employees, employee candidates, service providers, visitors of the CFCU and the other third parties in accordance with the Turkish Constitution, international conventions, the Law on the Protection of Personal Data No. 6698 and the other relevant legislation and determines as a priority to ensure that the relevant persons exercise their rights effectively.

Works and transactions regarding the storage and disposal of personal data are executed in accordance with this Policy prepared by the UNIT in this direction.

2. Scope

The personal data belonging to employees, employee candidates, service providers, visitors of the CFCU and the other third parties are within the scope of this policy and this policy is applied to all activities related to personal data processing and in all recording environments where personal data belonging to or managed by the CFCU, without prejudice to the relevant legislation.

In cases where hesitations or the unclear points are present in this Policy and in cases where the Policy is not sufficient, it is acted in line with other policies applied in the CFCU and the relevant legislation.

Unless otherwise stated in the policy, personal data and sensitive personal data will be collectively referred to as "Personal Data".

3. Definitions and Abbreviations

* Recipient Group: The category of natural or legal persons to whom the personal data is transferred by the Data Controller.

* Explicit Consent : Consent on a particular subject, based on information and expressed with free will.

* Anonymization: Making personal data incapable of being associated with an identified or identifiable natural person under any circumstances, even by matching with other data.

* Employee : Staff of the Central Finance and Contracts Unit (CFCU).

* EDMS: Electronic Document Management System.

* Electronic Media: Environments where personal data can be created, read, changed and written by electronic devices.

* Non-Electronic Media: All written, printed, visual etc. medias other than electronic media.

* Service Provider: A natural or legal person who provides services within the framework of a specific contract that is issued with the CFCU.

* Data Subject : A natural person whose personal data is being processed.

* Related User: People who process personal data within the organization of the data controller or in line with the authorization and instruction received from the data controller, excluding the person or unit responsible for the technical storage, protection and backup of the data.

* Disposal: Erasure, destruction or anonymization of personal data.

* (Applicable) Law: Law on Protection of Personal Data No. 6698.

* Recording Media: Any media where personal data is processed wholly or partially automatically or non-automatically, provided that it is a part of any data recording system.

* Personal Data: Any information related to an identified or identifiable natural person.

* Personal Data Processing Inventory: The inventory that data controllers have created by associating the personal data with; personal data activities carried out by them depending on their business processes, the purposes of processing, the data category, the transferred recipient group and the data subject group, while explaining the maximum period required for the purposes for which the personal data is processed, the personal data intended to be transferred to foreign countries and the measures taken regarding data security.

* Processing of Personal Data: Obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or blocking the utilization of such data completely or partially by automatic means or non-automatic means provided that it is a part of any data recording system.

* Board: Personal Data Protection Board.

* Sensitive Personal Data: Any data of race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, costume and clothing, membership to associations, foundations or unions, health, sexual life, criminal convictions and security measures and biometric and genetic data of individuals.

* Periodic Disposal: The erasure, destruction or anonymization process, which will be carried out ex officio at repetitive intervals specified in the personal data storage and disposal policy, in the event that all of the personal data processing conditions in the Law are eliminated.

* Policy: Policy on Storage and Disposal of Personal Data.

* Data Processor: Natural or legal person who/which processes personal data based on the authority granted by and on behalf of the data controller.

* Data registry system: The registration system in which the personal data is structured and processed according to certain criteria.

* Data Controller: The natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data registry system.

* Data Controllers' Registry Information System: Information system that is accessible through the Internet, established and managed by the Presidency, that data controllers will use for their application to the Registry and in the other operations related to the Registry.

* VERBIS: Data Controllers' Registry Information System.

* Regulation: Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated 28 October 2017.

4. Distribution of Responsibilities and Roles

The data controller is the Central Finance and Contracts Unit (the Unit). All managers and employees of the Unit provides active support in taking technical and administrative measures in all environments where sensitive personal data is processed, in taking adequate measures determined by the Personal Data Protection Authority about processing sensitive personal data, in order to prevent unlawful processing of sensitive personal data, to prevent unlawful access to sensitive personal data and to ensure that sensitive personal data are stored in accordance with the law, through training and awareness raising, monitoring, continuous inspection and the proper implementation of the technical and administrative measures taken within the scope of the Policy.

The distribution of the titles, departments and job descriptions of those involved in the storage and disposal processes of personal data is given in the Table 1.

Table 1: Role distribution of storage and disposal processes

Title	Department	Duty
PAO-CFCU Director	Central Finance and Contract Unit	Responsible for the employees to act in accordance with the Policy.

Information and Data Management Structure	Information and Data Management Structure	Responsible for the coordination of these functions: preparation, development, execution, publication and updating of the Policy in relevant environments.
All Other Departments	Other Departments/Sections	Responsible for the execution of the Policy in accordance with their duties, for performing the work and transactions required by the Policy.

5. Recording Media

Personal data are stored safely by the Unit in the environments listed in the Table 2, in accordance with the law.

Table 2: Personal data storage environments

Electronic Mediums	**Non-Electronic Mediums**
- Servers (Domain, backup, email, database, web, file sharing, etc.) - Software (office software, portal, EDMS, BELGENET etc.) - Information security devices (security wall, intrusion detection and prevention system, daily record file, antivirus, etc.) - Personal computers (desktop, laptop) - Mobile devices (Telephone, tablet, etc.) - Optical disks (CD, DVD, etc.) - Removable memory devices (USB, Memory Card, etc.) - Printer, scanner, photocopier	- Paper, - Manual data recording systems (inquiry forms, visitor book, etc.) - Written, printed, visual media

6. Explanations Regarding Storage and Disposal

Personal data belonging to employees, employee candidates, visitors, real persons from institutions and organizations served under contracts and protocols and the personal data belonging to the third parties involved as service providers and employees of institutions or organizations are stored securely and destroyed in accordance with the Law by the Unit.

As per the provisions of the third paragraph of the Article 7 of the aforementioned Regulation, all processes regarding the erasure, destruction and anonymization of personal data are recorded and these records are kept for at least 3 (three) years, excluding other legal obligations.

Within this scope, the following detailed explanations on storage and disposal are stated respectively.

6.1 The Explanations on Storage

The concept of "personal data processing" is defined in the Article 3 of the Law; it is remarked in the Article 4 of the law that the personal data processing should be "related to the processing purpose, limited, temperate and the personal data processed should be kept for a time required only for the processing purpose or for a period stipulated in the relevant legislation"; in the Articles 5 and 6 of the Law “the conditions of personal data processing” are stated as well.

Accordingly, pursuant to the activities of the Unit, the personal data is kept for a period stipulated in the relevant legislation or a period convenient for our processing purposes.

6.1.1 Legal Ground for Storage

The personal data processed pursuant to the activities of the Unit are kept for a period stipulated in the relevant legislation in the Unit. Within this scope, the personal data;

- Personal Data Protection Law No 6698,
- Turkish Code of Obligations Law No 6098,
- Tax Procedure Law No 213,
- Income Tax Law No 193,
- Law of the Central Finance and Contract Unit on the Employment and Budget Principles No 5671,
- Travel Expense Law No 6245,
- Public Procurement Law No 4734,
- Civil Servants Law No 657,
- Social Security and General Health Insurance Law No 5510,
- Regulation of publications on the internet and suppression of crimes committed by means of such publications Law No 5651,
- Public Financial Management and Control Law No 5018,
- Occupational Health and Safety Law No 6361,
- Right to information act Law No 4982,
- Exercise of the right to petition Law No 3071,
- Labour Law No 4857,
- Higher Education Law No 2547,
- Retirement Fund of Civil Servants Law No 5434,
- Social Services Law No 2828,
- Memorandum of Understanding on the Establishment of a Central Finance and Contracts Unit (CFCU) Between the Government of Turkey and the European Commission,
- Regulation on Central Finance and Contracts Unit Staff,
- Regulation On Principles And Procedures To Be Followed In Government Correspondence No 6321,
- Regulation on Food Allowance for Civil Servants,
- Presidential Decree No. 1,
- Regulation on Right to information act,
- Regulation on Health and Safety Measures to be Taken in Workplace Buildings and Extensions,
- Regulation on Archive Services,
- Other secondary regulations in force pursuant to these laws,

and when necessary within the framework of other relevant legislation, is kept for the stipulated periods.

6.1.2 Purposes of Processing That Require Storage

The Unit keeps the personal data being processed within the scope of its activities for the purposes indicated below;

- Carrying out the operations of human resources,
- Providing communication within the Unit,
- Providing security within the Unit,
- Ensuring the execution of operations and work processes within the Unit,
- Enabling to do statistical studies,
- Enabling to perform works and transactions arising from the contracts and protocols signed,
- Within the framework of the VERBIS; identifying the preferences and requirements of employees, data controllers, contact persons, data controller representatives and data processors, arranging the services accordingly and updating them when required,
- Ensuring the fulfillment of legal obligations required or mandated by the legal regulations,
- To contact with real / legal persons who have a business relationship with the UNIT,
- Making legal reporting,
- Managing processes of call center,
- Obligation of proving in case of a legal disputes that may arise later on,
- Ensuring the execution of audit/ internal audit/ inquires/ intelligence operations.

6.2 Reasons for Disposal

Personal data is erased, destroyed or anonymized by the UNIT upon the request of data subject or ex officio in following situations;

- Revising or repealing the provisions of the relevant legislation which constitutes the basis for processing,
- The disappearance of the reasons and/ or purpose that require processing or storage,
- In cases where the processing of personal data takes place providing that explicit consent is present, withdrawal of the explicit consent by the data subject,
- Approval of the data subject's application on erasure and destruction of her/his personal data within the framework of the rights of data subjects stipulated in the Article 11 of the Law by the Unit,
- In cases when, the UNIT rejects the data subject's application regarding erasure, destruction and anonymization of her/his personal data, the reply of the Unit is found insufficient by data subject or failure to respond within the period stipulated in the Law by the Unit; application of data subjects to the Board for complaint and acceptance of this application by the Board,
- Expiration of the maximum period of time required for the storage of personal data and absence of conditions to justify the storage of personal data for a longer period.

7. Technical and Administrative Measures

By the Unit;

- In order to keep personal data safe, prevent the illegal processing and accessing of them, the technical and administrative measures pursuant to the Article 12 of the Law,
- In order to destroy the personal data in accordance with the legislation, the measures pursuant to the Article 7 of the Law and relevant regulations,
- Pursuant to the 4th paragraph of the Article 6 of the Law, the adequate measures for sensitive personal data to be determined by the Board,

are taken.

7.1 Technical Measures

Related with the personal data processed, the technical measures taken by the Unit are listed below;

- The risks, threats, vulnerabilities and bugs (if any) within the information systems of our Unit are revealed by the penetration tests and necessary precautions are taken.
- As a result of information security incident management with real-time analysis, risks and threats that can affect the continuity of information systems are constantly monitored.
- Accesses to information systems and authorization of users are done by the security policies through the access & authority matrix with the corporate active directory.
- The necessary precautions are taken for the physical security of information system equipment, software and data of the Unit.
- In order to provide security of the information systems against the environmental threats, the measures regarding hardware (access control system that allows only authorized personnel to enter the system room, 24/7 employee monitoring system, ensuring the physical security of the edge switches that constitute the local area network, fire extinguishing system, air conditioning system etc.) and the measures regarding software (firewalls, attack prevention systems, network access control, systems that prevent harmful software etc.) are taken.
- In order to prevent the illegal processing of personal data the risks are detected, taking the suitable technical precautions for these risks is provided and technical controls are carried out for these measures taken.
- By recording the accesses to the storage mediums where personal data is located, the inappropriate accesses and access attempts are kept under control.
- In order that deleted personal data becomes inaccessible and non-reusable by the relevant users, the necessary precautions are taken by the Unit.

- By surveillance of the security vulnerabilities, the appropriate security patches are installed and the information systems are kept up-to-date.
- The use of passwords within the software utilized by the Unit are allowed according to the section of 'Password Policies' PIN Q.3.4 of Handbook of the Unit.
- The secure record keeping (logging) systems are used in electronic mediums where personal data are processed.
- Data backup programs, which provides safe storage of the personal data, are used.
- Accessing to the personal data stored within the electronic or non-electronic mediums are limited according to the principles of access.
- By using the security protocol (HTTPS), it is encrypted with SHA 256 bit RSA algorithm to access the web page of the Unit.
- A separate policy has been determined for the security of sensitive personal data, and the provisions of this policy are also taken into account in transactions related to sensitive personal data.
- Trainings on the security of sensitive personal data are provided to the staff who are involved in the processes of sensitive personal data, the confidentiality agreements are signed and the authorizations of the users who have access to data are defined.
- The electronic mediums in which the sensitive personal data are processed, stored and/or accessed are preserved by using cryptographic methods, the cryptographic keys are kept in secure mediums, all records of transactions are logged, the security updates of the mediums are constantly monitored. It is ensured that the necessary security tests are performed/ having them performed and the results of these tests are recorded.
- The adequate security measures are taken for the physical mediums in which sensitive personal data is processed, stored and/or accessed, and unauthorized logins and logouts are prevented by ensuring the physical security.
- In case that the sensitive personal data needs to be transferred via e-mail, they are transferred in encrypted form or via the account of registered electronic mail (REM). In case of necessity to transfer via the mediums like portable memory, CD and DVD, it is encrypted with cryptographic methods

and the cryptographic key is kept in a different medium. In case of transferring between the servers located in different physical mediums, data transfer is carried out by establishing a VPN between servers or using the sFTP method. In case of necessity to transfer via paper medium, the necessary precautions are taken against the risks such as theft, loss or viewing of the document by unauthorized persons and the document is sent in a "confidential" format.

7.2 Administrative Measures

Related to the personal data processed, the administrative measures taken by the Unit are listed below;

- In order to improve qualifications of the staff, trainings are provided on prevention of illegal processing of personal data, prevention of illegal access to personal data, protection of personal data, communication techniques, technical knowledge and skills, the Law No. 657 and other relevant legislations.
- Confidentiality agreements are signed by the employees regarding the activities carried out by the UNIT.
- The disciplinary procedure to be applied for the employees who do not comply with the security policies and procedures is followed in line with the registry and discipline provisions of the Civil Servants Law No. 657.
- Before initiating the process of personal data, the obligation to inform data subjects is fulfilled by the Unit.
- The inventory for personal data processing is prepared.
- The inspections/audit missions within the Unit are carried out periodically and randomly.
- Trainings on information security are provided for employees.

8. The Technics/ Methods for Disposal of Personal Data

At the end of the period stipulated by the relevant legislation or the storage period required for the processing purpose, by the Unit, ex-officio or upon the application

of data subject, personal data is selected to be sent for periodic destruction by at least 1 personnel assigned in the relevant department and is destroyed by the following techniques in accordance with the provisions of the relevant legislation. By taking into account the information in their own inventory; process, periodic follow-up/control, work and transactions regarding the disposal are under the responsibility of each department within the Unit and the follow-up is also carried out by the departments themselves. When necessary, it will be ensured that the relevant process is carried out in consultation with the Information and Data Management Structure. The issues specified in the Article 9 are also taken into consideration during in the transactions to be made within this scope.

8.1 Erasure of Personal Data

Erasure of personal data is the process of making personal data inaccessible and non-reusable for the relevant users.

The data controller is obliged to take all necessary technical and administrative measures to render the erased personal data inaccessible and non-reusable for the relevant users.

Personal data is erased by the methods given in Table-3.

Table 3: Deletion of Personal Data

Mediums in Which Data is Recorded	Explanations
The Personal Data in Servers	The system administrator removes the access authorization of the relevant users for the personal data in the servers of which the required storage period has expired, hence erases this personal data.
The Personal Data in Physical Mediums	The personal data in physical medium of which the required storage period has expired is rendered inaccessible and non-reusable in any way for the employees except for the director who

	is responsible of the document archive of the Unit. In addition, darkening (blackening) process is applied by drawing/painting/wiping in a way to render unreadable.
The Personal Data in Portable Mediums	The personal data in flash-based storage medium of which the required storage period has expired is encrypted by the system administrator and is kept in safe environments with encryption keys by giving the access authorization to the system administrator only.

8.2 Destruction of Personal Data

Destruction of personal data is the process in which personal data becomes inaccessible, unrecoverable and unusable by anyone in any way.

The data controller is obliged to take all necessary technical and administrative measures regarding the destruction of personal data.

Personal data is destructed by the methods given in Table-4.

Table 4: Destruction of Personal Data

Mediums in Which Data is Recorded	Explanations
The Personal Data in Physical Mediums	The personal data in paper medium of which the required storage period has expired are destroyed irreversibly in the paper shredders.
The Personal Data in Optical / Magnetic Mediums	The personal data in optical/magnetic mediums of which the required storage period has expired are destroyed by physical means of melting, burning or pulverizing. In addition, magnetic media is passed through a special device and exposed to a high magnetic

	field, in order to render the data on it unreadable.

8.3 Anonymization of Personal Data

Anonymization is the process of rendering personal data impossible to link with an identified or identifiable natural person, even though matching them with other data.

To anonymize the personal data, personal data shall be rendered impossible to relate to identified or identifiable natural person, even by using appropriate techniques in respect of the recording medium and relevant field of activity, such as recovery of personnel data by the data controller or third parties and matching data with other data.

The data controller is obliged to take all necessary technical and administrative measures regarding the anonymization of personal data.

9. Periods for Storage and Disposal

The Unit keeps the personal data until the purpose of processing is no longer valid or until the period stipulated by the relevant legislation. Accordingly, it is being followed up/ examined in the relevant legislation whether a storage period for the data is foreseen or not. In the event that the period expires or the reasons that require processing annuls, the personal data is disposed (erasure, destruction or anonymization) by the most appropriate method according to the mediums in which the data is stored.

When necessary, updates on the relevant storage periods are realized.

The personal data of which the storage periods has expired is determined by the personnel assigned in each department to be responsible for the disposal and the list of disposal is notified to the Information and Data Management Structure in writing. After finalization of the list for disposal, ex officio erasure, destruction or anonymization is carried out by the relevant department under the supervision of the Information and Data Management Structure.

10. Duration for Periodic Disposal

Pursuant to the Article 11 of the Regulation, the Unit has determined the duration for periodic disposal as 6 months, which is the maximum duration given in the Regulation. Accordingly, periodic disposal is carried out in the Unit in June and December every year.

11. Publication and Storage of the Policy

The policy is published in two different media; with wet signature (printed paper) and electronically, and is disclosed to the public on the website of the Unit. The printed paper copy is also stored in the Information and Data Management Structure file.

12. Update Period of the Policy

When required, this Policy is reviewed and the necessary sections are updated.

13. Enforcement and Revocation of the Policy

This Policy is deemed to have entered into force as of 01.01.2022. In the event that it is decided to be annulled, upon the decision of the Director of the CFCU, the wet signed old version/s of the policy is cancelled (with sealing of cancellation or by writing 'cancelled' on it) by the Information and Data Management Structure, then signed accordingly and kept for at least 5 years by the Information and Data Structure.