POLICY ON

PROTECTION, PROCESSING, STORAGE AND DESTRUCTION OF PERSONAL DATA

1. DEFINITIONS

Explicit Consent	Specific, informed and freely given consent, regarding a specific subject.
Anonymization	Rendering personal data to be impossible to link with an identified or identifiable real person, even though they are matched with other data.
Application form	The form set forth under Annex-1 of Clarification Text on Processing and Protection of Personal Data and Approval Form, prepared by the Data Controller in order that Data Owner can use the rights he/she has in accordance with Article 11 of the Law on Protection of Personal Data and can apply to the Data Controller for this purpose, and published on the SITE.
Audit Company	The persons authorized by the Public Oversight, Accounting and Auditing Standards Authority among professionals who have certified with public accountant license or independent accountant and financial advisor license to conduct independent audit, and who report in order to obtain sufficient and appropriate independent audit evidence that will provide reasonable assurance on the compliance and accuracy of the financial statements and other financial information of the Data Controller, by auditing and evaluating through books, records and documents and by applying the necessary independent auditing techniques stipulated in auditing standards.
Relevant User	The persons who process Personal Data within the organization of the Data Controller or in line with the authority and instruction received from the Data Controller, except for the person or unit responsible for the technical storage, protection and backup of Personal Data.
Law	Law No. 6698 on Protection of Personal Data.
GPDR	General Data Protection Regulation No. 2016/679.
Personal Data	Any type of information concerning an identified or identifiable ***real person***, including but not limited to name and surname, address, TR ID number, phone number, e-mail.
Board	The Personal Data Protection Board.
Authority	The Personal Data Protection Authority.
Destruction of Personal Data	Deletion, destruction or anonymization of personal data.

Processing of Personal Data	Processing of personal data is the series of operations that are carried out on personal data, such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or through non-automatic means only for the process which is a part of any data registry system.
Consortium	The consortium, which is composed of AESA, Global Rights Compliance which is under the leadership of AESA.
DG ENEST	Directorate-General for Enlargement and the Eastern Neighbourhood Negotiations Contracts and Finance Unit.
Special Category Sensitive Personal Data	The data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership of associations, foundations, civil society organizations, information relating to health, sexual life, convictions and security measures, and biometric and genetic data.
Policy	This Policy on Protection, Processing, Storage and Destruction of Personal Data.
Deletion	The process of rendering personal data inaccessible and unusable in any way for all relevant users.
Applications	The applications developed, owned or managed by the SITE, downloaded from the Google Play Store or AppStore and can be used on computers, mobile phones, tablets or other devices that the application enables/will enable.
Member	All non-governmental organizations (associations, foundations, non-profit cooperatives, civil society networks and platforms, Civil initiatives, communities, networks, City councils, Trade unions, non-profit companies, Bar Associations, Professional organizations, civil society units or centers of Universities working in the field of rights) and real persons who are internet users registered to MIS and/or E-bulletin and/or the programs carried out through the SITE.
Data Processor	The real or legal person who processes personal data on behalf of the data controller upon its authorization.
Data Registry System	The registry system which the personal data is registered into through being structured according to certain criteria.
Data Owner	Representatives of the sivil society organization who register to the SITE on behalf of organization and referred to as Member, members and employees of civil society organizations; real persons and all other Site users real persons, all of whose personal data is processed.

Data Controller	AESA, who determines the purposes and means of processing personal data, and who is responsible for the establishment and management of the data recording system.
ETKİNİZ	ETKINIZ – III EU Programme managed by the Data Controller.
SITE	Website on URL: http://etkiniz.eu/ and ETKİNİZ management.
MIS	ETKINIZ- III Management Information System (MIS).
Destruction	The process of rendering personal data inaccessible, unrecoverable and unusable in any way for any person.

2. PURPOSE OF POLICY ON PROTECTION, PROCESSING, STORAGE AND DESTRUCTION OF PERSONAL DATA

The purpose of this Policy is to inform the ***real persons*** whose data is processed by the SITE as Data Controller regarding the process, form and purposes of collecting, processing, storing, protecting and destroying their personal data, and their rights and methods of exercising their rights in accordance with the Law.

3. SCOPE AND AMENDMENT OF POLICY

This policy includes information in accordance with the Law and other legislation on personal data and entered into force on the date it was published on the SITE. The policy may be updated from time to time due to legal changes, changes that may occur in the Data Controller's process of Personal Data processing or for other reasons. Updates will become valid from the date of publication of the new Policy on the SITE.

4. CONDITIONS OF PERSONAL DATA PROCESSING OPERATION

Processing of Personal Data is the series of operations that are carried out on personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or through non-automatic means only for the process which is a part of any data registry system.

Personal Data cannot be processed without the explicit consent of the Data Owner in accordance with Article 5 of the Law. However, in accordance with the same article, it is possible to process personal data without requiring the explicit consent of the Data Owner in the presence of one of the following conditions. In the event that:

- It is explicitly provided for by the laws,
- It is mandatory for the protection of life or to prevent the body integrity of a person or any other person, in cases where that person cannot express consent due to physical disability or whose consent is legally invalid,
- Processing of personal data belonging to the parties of a contract is necessary, provided that it is directly related to the establishing or fulfilment of that contract,

- It is mandatory for the data controller to fulfil its legal obligations,
- The data is made available to the public by the Data Owner,
- Data processing is mandatory for the establishment, exercise or protection of any right,
- It is mandatory for the legitimate interests of the Data Controller, provided that such processing shall not violate the fundamental rights and freedoms of the Data Owner.

5. PROCESSING OF SPECIAL CATEGORY SENSITIVE DATA

These are the data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership of associations, foundations, civil society organizations, information relating to health, sexual life, convictions and security measures, and biometric and genetic data.

According to the Article 6 of the Law, it is prohibited to process the special category personal data without explicit consent of the data owner. However, personal data, excluding those relating to health and sexual life, may be processed without requiring explicit consent of the Data Owner, in the cases provided for by laws.

Personal Data relating to health and sexual life may only be processed without explicit consent of the data subject, by persons under an obligation of confidentiality or by authorised institutions and establishments for the purposes of protection of public health, protective medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

It is stipulated that adequate measures determined by the Board are also taken while processing Special Category Personal Data.

6. GENERAL PRINCIPLES OF PROCESSING PERSONAL DATA

Pursuant to Article 4 of the Law, Personal Data can only be processed in accordance with the procedures and principles stipulated in the Law or other laws. Compliance with certain principles during the processing of Personal Data is stipulated by the same article.

In this context, your personal data are processed in accordance with the following principles:

- **Lawfulness and conformity with rules of bona fides:** The Data Controller does not collect or process Personal Data without the knowledge of the Data Owner, and processes Personal Data in accordance with the legal system, the Law and the relevant legislation.
- **Accuracy and being up to date, where necessary:** The Data Controller makes the necessary effort to ensure that Personal Data is accurate and up to date. In this context, she/he keeps the channels that will provide this situation open in order to ensure the accuracy and update of the data and ensures the correction of the data upon the application of the Data Owner or ex officio upon detection.
- **Being processed for specific, explicit and legitimate purposes:** The purposes of the Data Controller for processing Personal Data are clearly determined as a requirement of the obligation to inform. The Data Controller processes Personal Data for legitimate purposes in accordance with the Law, in connection with the works and/or services it provides.
- **Being relevant with, limited to and proportionate to the purposes for which they are processed:** The Data Controller processes Personal Data for specific, explicit and legitimate purposes. In this context, the Data Controller ensures that the data is collected for the purposes

specified in this Policy or in the consent to be obtained from the Data Owner *(Explicit Consent)* and kept for the period required for the purpose and avoids the processing of Personal Data that are not related to and/or needed for the realization of the purpose, limits the processed data only to what is necessary for the achievement of the purpose.

- **Being retained for the period of time stipulated by relevant legislation or the purpose for which they are processed:** If there is a certain period stipulated in the relevant legislation for the storage of Personal Data, the Data Controller complies with this period. If such a period has not been determined, Personal Data is kept only for the period necessary for the purpose for which it was processed.

7. PROCESSED PERSONAL DATA

7.1. The ***real persons*** whose Personal Data may be processed by the SITE are explained and categorized in detail below.

Data Owner	**Descriptions**
Applicant	Real persons who submit questions, requests, suggestions, complaints and applications including those related to personal data by applying to the SITE in written, verbal or electronic form. Other data owners mentioned in this categorization may also be applicants.
Employee/Personnel	The persons working on the payroll of the Member or within its body and students/graduates who receive internship (compulsory/optional) training within the Member, regardless of whether they are bound by an employment contract or not.
Representative	The consultants, members and representatives of Civil Society Organizations that are members of the SITE.
Real Persons, Companies, Experts, Consultants Providing Services	Real persons who provide services to the SITE, whether within the scope of a contract or not. Subcontractors are also considered in this context.
Cooperated Real Persons	The real person merchants who undertake the execution of a certain work with ETKİNİZ - III and share the earnings as a result of this work.
Related People of Cooperated Company	The shareholders/partners, officials and employees of real or legal persons with whom ETKİNİZ – III cooperates.
Participant	The real persons participating in activities such as events, competitions and trainings organized by the SITE.
Related People of the MEMBERS	The shareholders/partners, officials, employees, members and representatives of SITE Members.

Shareholders	The real or legal persons holding shares in Data Controller member companies.
Consortium Official	Real persons who are in the senior management of the Consortium and its members and/or authorized to represent the Consortium. Board members are considered within this scope.
Application User	Real persons who download/use Applications, developed and made available by the Data Controller, on their mobile operating system device.
Visitor	All real persons who physically come to the Data Controller's workplace to provide or receive a product, service, service or not, and real persons who use the Website whether they are a member or not, record their data there, submit their data through the Website or whose data collected in accordance with the terms of use of the Website. Other data owners mentioned in this categorization may also be Website visitors.

7.2. Your personal data that is provided by yourselves during the registration to the SITE and/or within the scope of the performance of the Service and which may be subject to processing, are given below, as examples:

Identity Data	Name, surname, date of birth, country of birth, city of birth, sex, civil status, citizenship, Turkish Republic Identity Card information (Turkish Republic Identity Number (TRIN), serial number, certificate number, father's name, mother's name, place of birth, city, county, quarter, volume number, house range number, individual range number, section number, page number, registration number, place of delivery, reason of delivery, delivery date, maiden name), copy of birth certificate, passport number.
Communication Data	Work/mobile telephone numbers, open address information, e-mail (extension, corporate e-mail), social media account information, fax number
Special Category Sensitive Personal Data	Information about civil society organisation that he/she is a member of, such as Union, Association, Foundation, etc., status of being an ex-convict/criminal record, disability status/definition/percentage, religion, health information, blood type, health reports, association/foundation memberships, Social Security Premiums and taxes paid
Training Data	Educational background, certificate and diploma information, foreign language information, trainings and skills, CV, courses taken.

Audio-Visual Data	Photographs, sound recordings, video recordings of real person.
Performance and Career Development Data	Trainings and skills, professional activities, seniority, experience, training history (where and when it is received), information in which fields he/she worked, signed participation form, company and department information.
Other	Copy of driver's license, license plate, information that Data Owner grants approval to be shared through social media accounts if he/she connects through them, information about surfing and clicking on the site, information about the location where he/she opens the application, internet access logs, input-output logs, cookie policy, bank account number (IBAN and BIC), statement that it does not have the exceptions referred to in Articles 136-141 of the European Commission Financial Regulation, name and contact details of the reference persons.

8. COLLECTION METHODS OF PERSONAL DATA

The Data Controller collects and processes Personal Data in accordance with the regulations of this Policy, the Law and other relevant legislation, by means of written, verbal, electronic means, through audio/visual records or physically in contact with the Data Owner.

Data collection process can be carried out in the following ways:

i) Through digital media of third parties including e-mail, Website and Applications or a software,

ii) Through means such as contracts, applications, forms, call center, remote support, cookies on the SITE, business card, phone, or

iii) Through face-to-face interviews with the Data Owner.

9. PURPOSE OF PERSONAL DATA PROCESSING

The Data Controller processes Personal Data for specific, explicit and legitimate purposes. In this context, Personal Data can be processed for the following purposes:

9.1. Pursuant to 4th, 5th and 6th Articles of the PDPL, your personal data may be processed by the Data Officer, within the framework of his legal obligation arising from the relevant legislation, especially the Law. No. 5651 on Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication and the second relevant legislation, the Law No. 6563 on Regulation of Electronic Commerce and the second relevant legislation, Turkish Criminal Code No. 5237 and Law No. 6698 on Protection of Personal Data in order to achieve the purpose of ETKİNİZ, to provide you with better service and support; as;

a. Lawful and conforming the rules of bona fides,
b. Accurate and up to date, where necessary,
c. For specific, explicit and legitimate purposes,
d. Relevant with, limited to and proportionate to the purposes for which they are processed
e. According to the period of time stipulated by relevant legislation or required for the purpose they are processed.

Your personal data mentioned above will be processed and stored by taking security measures based on your explicit consent in connection with the activities of the SITE listed in article 9.2 below in order for you to benefit from the advantages of membership to the SITE and/or the e-bulletin on the condition that it is not used outside the purposes and scope specified below with this Document.

- To confirm the credentials of the member through the SITE and/or E-bulletin and/or programs carried out by the SITE,
- To record the address and other necessary information for communication,
- To communicate, provide necessary information and convey questions to the members of MIS and/or E-bulletin and/or the programs carried out within the scope of the activities of the SITE,
- To arrange all records and documents that will be the basis for processing in electronic media (internet / mobile etc.) or on paper,
- To be able to provide information to public officials on public security issues upon request and in accordance with the legislation,
- To increase the satisfaction of SİTE users and the members of MIS and/or E-bulletin and/or the programs carried out within the scope of the activities of the SITE, to organize surveys in electronic and/or physical environment,
- To be able to offer suggestions to MIS and/or E-bulletin members by our contracted institutions, solution partners and third party internet channels and digital programs that we are a member of, to inform MIS and E-bulletin members about our services,
- To be able to evaluate the complaints and suggestions of the members regarding the activities,
- To be able to fulfill our legal obligations and to exercise our rights arising from the current legislation,
- To prevent fraud and other illegal activities.

9.2. SITE Activities

a. Human Rights Monitoring Support: It is designed to support new and current human rights monitoring initiatives based on international human rights standards. With this support, it will be possible for Members to design and implement their own human rights monitoring works.

b. Support of Access to International Human Rights Mechanisms: It provides support for Members directly targeting international human rights mechanisms for the purposes of reporting and advocacy. With regards to human rights monitoring, it is designated to organise international study visits between Turkey, EU member countries and candidate countries and European Neighbourhood and Partnership Instrument (ENPI) countries, examine good practices on site and support activities of participation to events with items indicated on the SITE in detail. This support category provides a rapid opportunity for members wishing to prepare a report on different international human rights mechanisms. Meeting, travel, translation and other logistic needs necessary for preparing this report can be met with this support category. Besides, Members can also use this support to easily access international human rights mechanisms by participating in meetings or sessions where these reports are discussed and organising one-to-one interviews.

c. Organisation of Training Programme: Different training programmes that will be needed by members for monitoring human rights are organised by ETKİNİZ and announcements regarding these trainings can be found on social media accounts and in announcement section of the SITE.

d. News: Data, announcements, report, studies, etc. published by institutions, organisations, foundations, associations and bodies with regard to improvement and protection of human rights in Turkey and in the world are presented to members by filtering this information from a remarkably comprehensive database.

e. ETKİNİZ Non-Key Pool: In accordance with Members' needs, support of experts having different levels of know-how, expertise and experience is provided. In addition to this, ETKİNİZ Non-Key Pool is utilised in order to create and implement learning opportunities covering training programmes and contents under different subject titles provided for Members.

f. ETKİNİZ EU Programme Help Desk: ETKINIZ EU Programme Help Desk provides service from 13:30 to 16:30 each weekday. This unit which provides service through telephone and e-mail replies questions about the programme.

9.3. Other purposes:

a. Communicating by the SITE for satisfaction measurement surveys,

b. Management of judicial/administrative processes, responding to requests from public institutions, fulfilling legal obligations depending on legal regulations, resolving legal disputes,

c. Providing contact/communication,

d. Introduction of Data Controller's employees through social media posts,

e. Conducting job interviews, evaluating job applications,

f. Establishment, execution, and termination of the business relationship/employment agreement,

g. Reporting within the framework of cooperation,

h. Making participant registration in case of participating in an organization on behalf of ETKİNİZ,

i. Creating personal data inventory,

j. Creating and tracking visitor records,

k. Ensuring the internal and environmental security of the Data Controller and the security of the SITE and Applications,

l. Usage analysis of the Website,

m. Evaluating and responding to all questions, requests, suggestions, complaints and applications submitted in writing, verbally or electronically, including those related to personal data.

10. PERSONAL DATA RECORDING MEDIA

Personal Data collected by the Data Controller can be recorded in a wide variety of media, depending on the nature of the data, the purposes of the processing, and the frequency of use. In this context, the Data Controller can save Personal Data in the following media:

- Media such as paper, software, cloud, the central server, portable media, database;
- Peripheral systems such as network devices, flash-based media, magnetic tape, magnetic discs, mobile phones, optical discs, printers, door entry/security systems.

11. TRANSFER OF PERSONAL DATA

11.1. Transfer of Personal Data in Country

According to Article 8 of the Law, as a rule, Personal Data cannot be transferred without explicit consent of the Data Owner.

However, pursuant to Article 4 of the Policy, in the event that there is one of the situations in which the explicit consent of the Data Owner is not required, it is possible to transfer the Personal Data to third parties in the country without the explicit consent of the Data Owner.

11.2. Transfer of Personal Data Abroad

According to Article 9 of the law, as a rule, Personal Data cannot be transferred without the explicit consent of the Data Owner.

However, if one of the following situations exists, Personal Data may be transferred to third parties abroad without the explicit consent of the Data Owner.

- Presence of one of the situations in which the consent of the Data Owner is not required as specified in the Articles 4 or 5 of this Policy,
- Adequate protection is provided in the foreign country where Personal Data will be transferred,
- Data controllers in Turkey and in related foreign countries guarantee sufficient protection in writing and the Board has authorized such transfer, where sufficient protection is not provided.

Countries providing sufficient protection are determined and announced by the Board.

Without prejudice to the provisions of the international agreements, Personal Data can only be transferred abroad with the permission of the Board in cases where the interests of Turkey or the Data Owner will be seriously harmed, only with the opinion of the relevant public institution or organization.

11.3. Third Persons to Which Personal Data can be Transferred in Turkey and Abroad

Data Controller can transfer Personal Data to the following third persons who can be a real or legal person in the country or abroad, in accordance with Articles 8 and 9 of the Law, in order to realize the purposes specified in Article 9 of this Policy:

- Consultants
- Affiliated Companies, Community Companies
- Cooperated Companies
- Tender and Contracting Authorities
- EU Delegation to Turkey
- Human Rights Joint Platform
- Consortium
- DG ENEST

Within the scope of the Program, personal data can be transferred to third parties in the country within the categories mentioned above, as well as to Consortium member companies residing abroad, and to DG ENEST in order to achieve the purpose of the Program. The clarification text published in accordance with the European Union General Data Protection Regulation and other relevant regulations on the transfer of your personal data to DG ENEST and the processing by DG ENEST is available at https://ec.europa.eu/europeaid/prag/annexes.do?chapterTitleCode=A.

12. PRIVACY AND SECURITY OF PERSONAL DATA

The SITE attaches importance to the privacy and security of Personal Data, and takes legal, technical and administrative measures to protect the Personal Data to the extent stipulated by the Law and the relevant legislation.

12.1. Reasons Requiring the Storage and Destruction of Personal Data

12.1.1. Legal, Technical and Other Reasons Requiring the Storage of Personal Data

In the event that the primary purpose of collecting Personal Data or, if any, the secondary processing basis specified in this Policy disappears, the Personal Data will continue to be stored by the Data Controller:

- In order to fulfill the legal responsibilities of the Data Controller that have arisen or may arise, and in accordance with the measures stipulated in the laws and/or the periods ordered,
- Data that is expected to be deleted and/or anonymized - in a way not ready for access ("live") in backup/archive and similar media for business continuity, prevention of data loss and ensuring data protection,
- Data to be destroyed by deletion, destruction, or anonymization - until the next periodic destruction

date at the latest.

12.1.2. Legal, Technical and Other Reasons Requiring the Destruction of Personal Data

- The disappearance of all purposes requiring the processing of Personal Data and the reasons requiring its storage,
- In cases where the processing of personal data takes place only on the condition of explicit consent, the person concerned withdraws his/her consent,
- In case that Data Owner requests the destruction of his/her Personal Data by using his/her rights mentioned in Article 11 of the Law and Article 16 of this Policy and the application is accepted by the Data Controller, or the request is approved by the Board as a result of a complaint to the Board upon the rejection of this request,
- In case the maximum period that requires the storage of Personal Data has passed and there is no condition that justify the storage of Personal Data for a longer period.

12.2. Measures Taken to Ensure Safe Storage of Personal Data and Preventing Unlawful Processing and Accessing

12.2.1. Technical Measures

- Access authorities to Personal Data are limited and access records are kept,
- In order to prevent unlawful intervention to Personal Data both from inside the SITE and from

outside, data recording media are protected by various software/hardware and passwords, especially virus protection programs,Necessary inspections are carried out to process Personal Data in accordance with the procedures and principles stipulated in the Law,

- Data recording media under the responsibility of the Data Controller are regularly subjected to security tests by expert organizations, and if a security vulnerability is detected, this vulnerability is corrected,

12.2.2. Administrative Measures

- Employees are provided with training on the relevant legislation to prevent unlawful processing and access to personal data and to ensure their storage.
- The Data Controller arranges confidentiality agreements with the personnel who process Personal Data or with third parties who access the data (such as consultancy and information processing services).
- Disciplinary procedure to be applied to employees who do not comply with security policies and procedures have been prepared and communicated to the personnel.
- Before starting to process personal data, the obligation to inform the persons concerned is fulfilled.
- Personal data processing inventory has been prepared.
- Periodic and random internal inspections are carried out.
- Information security training is provided to employees.
- Physical security measures are taken for the media where personal data is contained.
- In the documents received, special category sensitive personal data (such as religious data, blood type) are destroyed by the blackout method.
- In order to prevent unauthorized access to physical documents, the cabinets containing the documents are kept locked and the entrance and exit of the room, where the documents are located, are ensured to be controlled.
- If it is necessary to transfer Sensitive Personal Data through paper, necessary measures are taken against risks such as theft, loss or being seen by unauthorized persons and the document is sent in "confidential" format.
- Adequate security measures are taken in the physical environments where special category sensitive personal data is processed, stored, and/or accessed, and unauthorized entry and exit are prevented by ensuring physical security.
- A suitable system and infrastructure have been established by the Data Controller to notify the relevant person and the Authority in case Personal Data is illegally obtained by others.
- Necessary training has been provided to the personnel regarding which of the processed Personal Data requires Explicit Consent.

12.3. Measures Taken for the Legal Destruction of Personal Data

12.3.1. Technical Measures

- Destruction is carried out by knowledgeable technical personnel or under their supervision.

12.3.2. Administrative Measures

- Personal Data Protection Committee has been established and its functionality is ensured,
- Employees are trained and informed about the periodic and proper destruction of personal data,
- Regular inspections are carried out,

- In the contracts to be concluded with employees and third parties, provisions that sanction the non-destruction of data in accordance with the Law and other relevant legislation are added.

12.4. Personal Data Protection Committee

In order to carry out the processes of storage and destruction of Personal Data and to take the necessary actions in accordance with this Policy, a "Personal Data Protection Committee" has been established under ETKİNİZ, which consists of the persons whose title and positions are specified below.

Department and Title	**Role in the Committee and Description**
Project Coordinator	**Committee President**: Committee meetings, implementing and executing the policies, informing the Board of Directors regarding the process, following up the relations with the Personal Data Protection Board, and following up the Board Decisions,
Project Officer	**Human Resources Officer of the Committee:** Realization of the secretariat services of the committee, execution, and planning of human resources affairs
IT Manager	**IT Officer of the Committee:** Establishing, monitoring, implementing, destroying, and anonymizing IT systems, creating the necessary mechanisms for transfer in the country and abroad, ensuring the security of data, proposing, and implementation systems that provide data security.

The main duties of the committee are as follows:

- To prepare or have prepared policies regarding the protection, storage, processing and destruction of Personal Data and to put them into effect,
- To conduct or have internal SITE inspections to ensure compliance of the processes of protection, storage, processing and destruction of Personal Data with the Law and Policy, and to ensure that necessary measures are taken to eliminate any deficiencies or risks in this direction,
- To provide information to employees in order to ensure lawful process and destruction of Personal Data and to prevent unlawful access, to organize trainings when deemed necessary, or to ensure that employees participate in trainings organized by third parties,
- To evaluate the applications of the Data Owners, to provide coordination within the Consortium to respond to the applications and to ensure that the response is delivered to the Data Owner within the legal period,
- To follow the changes in the legislation regarding Personal Data personally, through Consultants or Service Providers, to ensure that actions are taken within the Consortium in order to comply with the new regulations,
- To provide the necessary coordination and communication in cases where communication with the Board is required.

12.5. Products and Services of Third Party Organizations

The support and services provided by ETKİNİZ - III, the SITE, and Applications, may contain and provide links to websites, products, and services operated by third party organizations that the Data Controller does not own and control. If you benefit from this website, products and services, your personal data may be transferred to third party organizations. The Data Controller does not give any guarantee or special commitment that the content, compliance, security, privacy policies and communication related to the accessed website, products and services will be maintained continuously. Before any action is taken, the security and privacy conditions of the companies in question should be read.

13. DESTRUCTION OF PERSONAL DATA

Although it has been processed in accordance with the provisions of the Law and other relevant laws, in the event that all reasons requiring its processing and storage are eliminated, Personal Data is deleted, destroyed, or anonymized by the Data Controller, either ex officio or at the request of the Data Owner.

13.1. Deletion of Personal Data

The deletion of Personal Data is the process of rendering personal data inaccessible and unusable for all relevant users.

The Data Controller can use the following methods to delete Personal Data, depending on the medium in which the data is recorded:

- Issuing a Command to Delete
- Blackout
- Removing the Related User's Access Rights on the Directory of the File
- Deleting Through Software
- Deleting through Database Command

13.2. Destruction of Personal Data

Destruction of personal data is the process of rendering Personal Data inaccessible, irreversible and unusable in any way by any person.

The Data Controller may use one or more of the following methods to destroy Personal Data, depending on the medium in which the data is recorded:

- De-Magnetizing
- Physical Destruction
- Overwriting
- Destruction through "Block Erase" Command
- Destruction with Paper Shredder
- Destructing All Copies of Encryption Keys

13.3. Anonymization of Personal Data

Anonymization of personal data is defined as rendering personal data impossible to link with an identified or

identifiable real person, even though matching them with other data.

In order for the Personal Data to be anonymized, it must become impossible for Personal Data to be associated with any identified or identifiable person in any way, even through the use of appropriate techniques in terms of the recording medium and the relevant field of activity, such as the return of the personal data and matching the data with other data by the third person or persons to whom the data is transferred or by the Data Controller.

The Data Controller can use one or more of the following methods to anonymize Personal Data:

- Removing Variables
- Removing Records
- Lower and Upper Limit Coding
- Partial Concealment
- Sampling
- Micro aggregation
- Data Swapping
- Noise addition
- K-anonymity
- L-diversity
- T-closeness

14. STORAGE AND DESTRUCTION PERIODS OF PERSONAL DATA

As a basic principle, the Data Controller retains the personal data on the basis of the period specified in the relevant laws and national/international legislation, if stipulated in these regulations. If a period of time is not regulated in the legislation regarding how long the personal data should be stored, the Personal Data are processed for the period required to be processed in accordance with the practices and commercial life practices of the Data Controller or the statute of limitations stipulated in the relevant laws, depending on the activity carried out while the Data Controller is processing that data, and then deleted, destructed or anonymized.

If the purpose of processing personal data has expired and the Data Controller has reached the end of their retention period in terms of the relevant legislation, Personal Data can only be stored for the purpose of providing evidence in possible legal disputes or for the purpose of asserting the right related to personal data or establishing a defense. In the determination of the periods here, the retention periods are determined based on the limitation periods for the assertion of the mentioned right and the examples in the requests made to the Data Controller on the same issues before, although the limitation periods have passed. In this case, the stored personal data is not accessed for any other purpose, and access to the relevant personal data is provided only when it is required to be used in the relevant legal dispute. Personal data is deleted, destroyed or anonymized after the period mentioned here expires.

Quality of Data	Storage Period	Periodic Destruction Time

Personal Data in the files regarding the processes carried out within the scope of the tender or activity	10 years from the date of program contract signature	Totally, in the month following the month in which 10 years period is completed
Records of the Data Owner whose proposal or grant request is not accepted	In case the grant request of the data owner is rejected, 5 years from the date of rejection	Periodically, within the month following the month when the 5 years period is completed, separately for each data
Personal Data in files regarding program implementation processes	10 years from the date of program contract termination	Totally, in the month following the month in which 10 years period is completed
Personal Data in the records of program income and expenses	7 years from the date the program's final payment is made	Totally, in the month following the month in which 7 years period is completed

In the event that the obligation to delete, destroy or anonymize arises due to the expiration of these periods, the Data Controller deletes, destroys or anonymizes the Personal Data in the first peri odic destruction process following this date.

15. RIGHTS OF THE DATA OWNER AND THE EXECUTION OF THESE RIGHTS

15.1. Rights of the Data Owner

The Data Owner has the following rights by applying to the Data Controller in accordance with Article 11 of the Law:

- To learn whether his/her personal data is processed or not,
- To request information regarding the process of his/her personal data, if processed,
- To learn the purpose of his/her data processing and whether this data is used for intended purposes,
- To know the third parties to whom her/his personal data is transferred in the country or abroad,
- To request correction of Personal Data in case of incomplete or incorrect processing and notifying this procedure to third parties to whom Personal Data is transferred,
- Although it has been processed in accordance with the provisions of the Law and other relevant legislation, in case the reasons requiring its processing disappear, to request the deletion or destruction of personal data and notifying this procedure to the third parties to whom the personal data has been transferred,
- To object to the occurrence of a result against the person itself by analyzing the processed data exclusively through automated systems,
- To request indemnification of the damage arising from the unlawful processing of her/his personal data.

15.2. Situations Where the Law is not Applicable and the Data Owner Cannot Exercise Her/His Rights

The provisions of the Law will not be applied in the presence of exceptional cases in accordance with the 1st paragraph of Article 28 of the Law. These exceptions are the following cases where:

- Personal data is processed by natural persons within the scope of purely personal activities of themselves

or of family members living together with them in the same dwelling provided that it is not to be disclosed to third parties and the obligations regarding data security are to be complied with;

- Personal data is processed for the purpose of official statistics and for research, planning and statistical purposes after having been anonymized;
- Personal data is processed for artistic, historical, literary or scientific purposes, or within the scope of freedom of expression provided that national defense, national security, public security, public order, economic security, right to privacy or personal rights are not violated or are processed so as not to constitute a crime;
- Personal data is processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorised and assigned by laws to ensure national defense, national security, public security, public order or economic security;
- Personal data is processed by judicial authorities or execution authorities with regard to investigation, prosecution, criminal proceedings or execution proceedings.

In accordance with paragraph 2 of Article 28 of the Law, the Data Owner cannot exercise his/her rights specified in Article 15.1 of this Policy, except for the right to demand indemnification of his/her damages, in the following cases where personal data processing:

- is required for the prevention of a crime or crime investigation;
- is carried out on the data which is made public by the data owner herself/himself;
- is required for inspection or regulatory duties and disciplinary investigation and prosecution to be carried out by the public institutions and organizations and by professional associations having the status of public institution, assigned and authorised for such actions, in accordance with the power conferred on them by laws;
- is required for protection of State's economic and financial interests with regard to budgetary, tax-related and financial issues.

15.3. Exercise Procedures of Data Owner's Rights

By filling out the application form in Annex-1 of the CLARIFICATION TEXT AND APPROVAL FORM for using your rights specified in Article 15.1 of this Policy, as Data Owner, you can personally submit a signed copy of the form to " Çankaya Mahallesi, Nergis Sokak No:2/5,Çankaya/ Ankara " with documents identifying your identity, or send the relevant form through a public notary, or transmit the form to info@etkiniz.eu from your email address previously notified to the Data Controller with a secure electronic signature or mobile signature. The application must include the following:

- Name, surname and signature, if the application is in writing,
- T.R identification number for citizens of the Republic of Turkey, nationality, passport number or identification number, if any, for foreigners,
- Residential address or workplace address for notification,
- Email address, telephone and fax number, if any, for notification,
- In case the Data Owner wishes to exercise this right through his/her proxy, a copy of the power of attorney containing special authority in this regard,
- Subject of the request.

15.4. Responding to Data Owner's Application

Requests sent with the form will be replied free of charge as soon as possible and within thirty days at the latest from the date the application is received by the Data Controller, depending on the nature of the request. However, if the transaction requires an additional cost, the fee in the tariff determined by the Board may be charged.

In cases such as incomplete or incorrect sharing of information, the request that is not expressed in a clear and comprehensible manner, the documents that support the request that are not submitted at all or as required in the application, absence of copy of the power of attorney for applications through proxy, the Data Controller may have difficulties in meeting the requests and the research process may be delayed. For this reason, it is important to comply with these issues in the exercise of the rights specified in Article 11 of the Law. Otherwise, the Data Controller will not be held responsible for any delays.

The legal rights of the Data Controller are reserved against false, untrue/unlawful and/or malicious applications.

15.5. Data Owner's Right to Lodge a Complaint

If the application is refused, the response is found insufficient or the request is not answered in time, the Data Owner has a right to lodge a complaint with the Board within thirty days as of he/she learns about the response of the Data Controller, or within sixty days as of the request date, in any case.