GLOBAL COMMUNITIES INC TURKEY REPRESENTATIVE OFFICE
PERSONAL DATA RETENTION AND DESTRUCTION POLICY

CONTENTS

GLOBAL COMMUNITIES INC TURKEY REPRESENTATIVE OFFICE
PERSONAL DATA RETENTION AND DESTRUCTION POLICY

1. INTRODUCTION

1.1. Purpose

This Personal Data Retention and Destruction Policy ("**Policy**") has been prepared for the purpose of determining the procedures and principles regarding the storage and disposal activities carried out by our Association Global Communities Inc. Turkey Representative Office ("**GLOBAL COMMUNITIES**" or "**Association**") which has the title of data controller pursuant to the Law on the Protection of Personal Data No. 6698 and the Regulation on the Deletion, Destruction or Anonymization of Personal Data, which was published in the Official Gazette dated 28 October 2017 and entered into force on 1 January 2018. The policy aims to provide information on the principles for determining the maximum time required for the purpose for which your personal data is processed, as well as the processes for deleting, destructing and anonymizing.

The works and procedures regarding the storage and destruction of personal data are carried out in accordance with the Policy prepared by our Association in this direction.

1.2. Scope

The scope of this Policy includes personal data of Association employees, donors, volunteers, needers, researchers, candidates, service providers, visitors and other third parties, and this Policy applies to all recording mediums where personal data owned by the Association or managed by the Association are processed, and for activities related to personal data processing.

2. DEFINITIONS

- **Explicit Consent:** Consent regarding a specific subject, informative and disclosed with free will.
- **Receiver Group:** The category of natural or legal persons to whom personal data is transferred by the Data Controller.
- **Electronic environment:** Environments where personal data can be created, read, changed and written with electronic devices.
- **Non-Electronic Environment:** All written, printed and other media other than electronic media.
- **Related User:** Persons who process personal data within the organization of the data controller or in accordance with the authorization and instruction received from the data controller, with the exception of the person or unit responsible for the technical storage, protection and backup of the data.
- **Destruction:** Deletion, destruction or anonymization of personal data.
- **Service provider:** Real or legal person providing services to our association within a certain contract.
- **Recording Medium**: Any medium where personal data are processed by non-automated means provided that being fully or partially automated or part of any data recording system

- **The Law on the Protection of Personal Data:** The Law on The Protection of Personal Data No. 6698.
- **Personal Data:** Any information about an identified or identifiable natural person.
- **Personal Data Processing Inventory:** Inventory detailed by the data authorities by explaining the personal data processing activities they carry out depending on the business processes, the maximum time required for the purposes of processing personal data, the data category, the group of recipients transferred and the group of data subject, and the personal data foreseen to be transferred to foreign countries, and measures taken for data security.
- **Processing of Personal Data:** All kinds of processes performed on data such as preventing, saving, storing, maintaining, modifying, reorganizing, disclosing, transferring, taking over, making available, non-classified, classifying or preventing personal data fully or partially automated or as part of any data recording system.
- **Anonymization Personal Data:** The process of making personal data unrelated to an identified or identifiable natural person under any circumstances, even by matching with other data.
- **Deletion Personal Data:** The process of deleting personal data, making personal data inaccessible and unusable for Related Users.
- **Destruction Personal Data:** The process of destructing personal data, making personal data in no way accessible, retrieved and reusable by anyone.
- **Council:** Personal Data Protection Council.
- **Global Communities/ Association:** Global Communities Inc. Turkey Representative Office
- **Special Quality Personal Data:** Individuals' race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, disguise and outfit, association, foundation or union membership, health, sexual life, criminal conviction and security measures and biometric and genetic data.
- **Periodic Destruction:** The process of deleting, destroying or anonymizing the personal data contained in The Law on the Protection of Personal Data, which will be performed manually at repeated intervals specified in the policy of storing and destroying personal data, if all the conditions of processing disappear.
- **Policy:** This Personal Data Retention and Destruction Policy.
- **Data Processor:** The natural or legal person who processes personal data on his/her behalf based on the authorization of the data controller.
- **Data Recording System:** Registration system where personal data is processed according to certain criteria.
- **Data Owner/Related Person:** Natural person whose data processed.
- **Data Controller:** 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 recording system..
- **Data Controllers Registry Information System /VERBİS**: The information system that Data Controllers will use for application to the Registry and other related transactions related to the Registry, which can be accessed over the internet, created and managed by the Personal Data Protection Authority.
- **Regulations:** Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette on 28 October 2017 and entered into force on 1 January 2018.

3. PRINCIPLES

The following principles in article 7 of the Regulation are complied with in the preparation, implementation and processing of personal data of the Policy.

- In the event that all the processing conditions of personal data in articles 5 and 6 of the PDPL disappear, the personal data will be deleted, destroyed or anonymized by the data officer or upon the request of the person concerned.
- In the deletion of personal data, the following principles listed in article 4 of the PDPL are fully followed:
    a) Being in compliance with law and honesty rules,
    b) Being accurate and up-to-date when necessary,
    c) Processing for specific, clear and legitimate purposes,
    d) Being related, limited and temperate for the purpose for which they are processed,
    e) Being preserved for the period required by the relevant legislation or for the purpose for which they are processed.
- The technical and administrative measures regulated under Article 12 of the PDPL are complied with.
- It acts in accordance with the decisions of the Council.
- All transactions regarding the deletion, destruction, anonymization of personal data are recorded and these records are kept for at least 3 years, excluding other legal obligations.
- The data officer chooses the appropriate method of deleting, destroying or anonymizing personal data ex officio unless a decision is made by the board. Upon the request of the person concerned, he / she will choose the appropriate method by explaining its reason.

4. RECORDING MEDIUMS

Personal data of you data owners are securely stored by the Global Communities in the environments listed in the table below, in accordance with other relevant legislation, in particular the PDPL provisions:

Recording Mediums:

- Office 365
- Podio
- Vismo.com
- SmarterASP.net
- TABLEU
- Device Magic
- SaasAnt for quickbooks
- QGIS
- ArcGIS
- Google Drive
- TimeSheet System
- IT Stack Db

- Active Directory
- Carbonite
- Sonicwall Firewall
- Ms Office
- Quick Books
- İş Bilgisayarı
- Surveilling System DVR
- Admin Db
- Power BI
- KOBO
- Fullcrum
- Ortak Alan
- File Server

Physical Medium:

- Archive
- Locked Unit Cabinets

5. EXPLANATIONS ON RETENTION AND DESTRUCTION

Personal data belonging to the employees, candidates, visitors and third parties, institutions or organizations with whom it is associated as a service provider are stored and destroyed by our association in accordance with the PDPL.

In this context, detailed explanations about storage and destruction are given below.

5.1. Explanations on Retention

In PDPL article 3, the concept of the processing of personal data is defined, it is stated that the personal data processed in article 4 should be connected, limited and measured for the purpose for which they are processed and should be maintained for the period stipulated in the relevant legislation, and in 5, the processing conditions of the personal data are counted.

Accordingly, within the framework of the activities of our Association, personal data are stored for a period specified in the relevant legislation or in accordance with our processing purposes.

5.2. Legal Reasons Requiring Retention

In our association, personal data processed within the scope of our activities are retained for the period stipulated in the relevant legislation (and relevant exceptions specified therein). In this context, personal data are retained;

- As long as the retention periods stipulated under other secondary regulations in force in accordance with the following laws
- The Law on the Protection of Personal Data No. 6698,

- Law of Associations No. 5253,
- Turkish Code of Obligations No. 6098,
- Social Security and General Health Insurance Law No. 5510,
- Tax Procedure Law No. 213,
- Law on Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications No. 5651,
- Occupational Health and Safety Law No. 6361,
- Right to Information Act No. 4982,
- Law on Exercise of the Right to Petition No. 3071,
- Labor Law No. 4857,
- Regulation on Blood and Blood Products No. 27074
- Blood and Blood Products Law No. 5624
- Regulation on Health and Safety Measures to be Taken in Workplace Buildings and Annexes

5.3. Processing Purposes Requiring Retention

Our association retains the personal data it processes within the framework of its activities for the following purposes.

Our Purposes of Personal Data Processing	Examples
Evaluation of potential donors, volunteers and trainers	Informing the prospective donor, submitting the donor registration form and donor inquiry form
Establishment and management of donor and volunteer relations	Collecting and evaluating the information of the volunteers who want to take part in the activities or activities organized by Global Communities, providing donor support and increasing resources through activities and campaigns carried out by Global Communities, transferring donations to the system (for both individual and corporate donors), receiving in-kind and cash donations, informing the candidate of the donor, identifying the donor candidate's identity, receiving donations, delivering donations to the required places, fulfillment of the requests of donors who want to update their credentials, control of payments, and checking whether they are in the list of people who should not be specifically taken for the services and products received.
Establishment and management of beneficiary relations	Determining the needs of those in need and their needs, evaluating demand forms from Global Communities branches, conducting financial aid to those in need, conducting cash aids
Execution and finalization of the contract process	Managing the procurement and invoicing process of our association, purchasing services and materials, establishing and executing contracts,

Our Purposes of Personal Data Processing	Examples
with our suppliers / business partners	ensuring post-contract legal transaction security, retaining the information after the contract, filling the form after the purchase of the goods, collecting the data of the people who received the goods, developing the service, evaluating the new technologies and applications, and determining and exercising the strategies of our Association, Providing training in processes related to managing operations (demand, proposal, evaluation, ordering, budgeting, contract), evaluating processes within the scope of the organization in terms of compliance and minimizing risks, standard of behavior, fraud, etc., conducting investigations, controlling financial operations and records, managing financial affairs, organizing tenders for outsourcing.
Conducting direct marketing processes	Making notifications about our activities via e-mail and telephone, making satisfaction surveys or evaluating your feedback, complaints and comments on social media, online platforms or other channels, giving information about the activities of the Global Communities to the participants in the activities organized by Global Communities.
Contact and support (upon your request)	Responding to requests for information regarding our association's activities, updating our records and database,
Compliance with legal obligations	With regulatory and supervisory agencies within the scope of the requirements and obligations determined to ensure that the legal obligations specified in the Law on the Protection of Personal Data are fulfilled as required or required by legal regulations, execution of tax and insurance processes, fulfilling our legal obligations arising from the relevant legislation especially Associations Law No. 5253, Law on Associations and Foundations' Relations with Public Institutions No. 5072, Law No. 5651 and other legislation, Law No. 6563 on Regulation of Electronic Commerce and other legislation, Turkish Criminal Code No. 5237 and Law on Protection of Personal Data No. 6698, execution of processes before official institutions, recording and information obligations, compliance and audit, audit and inspection of official authorities, following and finalizing our legal rights and cases, carrying out the necessary processes within the scope of compliance with the laws and regulations we are subject to, such as disclosure of data upon the request of the official authorities (sharing information with the Ministry of Family and Social Policies in the processes carried out regarding the beneficiaries, etc.),
Protection and security of association interests	Carrying out the necessary audit activities for the protection of the interests and interests of the Association, ensuring the legal security of the persons who are in contact with our Association, keeping CCTV records for the protection of the equipment and assets of the association, taking technical and administrative security measures, carrying out the necessary studies for the development of our activities, applying and auditing the workplace rules, planning and execution of social

Our Purposes of Personal Data Processing	Examples
	responsibility activities, protection of the reputation and trust of Global Communities economic enterprises, making all necessary interventions and taking precautions by reporting all incidents, accidents, complaints, lost stolen etc. situations occurring within the Global Communities facilities, transferring the rules to be followed for dangerous situations that may occur during maintenance and repair and measuring the professional competencies of subcontractors, ensuring the order of the entries and exits of Global Communities employees and obtaining necessary information in terms of security, performing our necessary inspections or fulfilling our reporting and other obligations determined by laws and regulations.
Planning and execution of association activities	Conducting communication, market research and social responsibility activities, managing power of attorney and authorization processes carried out by our Association for the purpose of determining, planning and implementing short, medium and long term policies of the Association, determining and implementing its strategies.
Reporting and audit	Ensuring communication with Global Communities economic enterprises, conducting necessary activities, internal audit and reporting processes
Protection of rights and interests	Defense against legal claims such as lawsuits, investigations, etc. filed against our association

5.4. Reasons Requiring Destruction

Personal Data, in such cases as

- Amendment or relevance of the relevant legislation provisions that constitute the basis for its processing,
- Elimination of the purpose that requires processing or storage,
- In cases where the processing of personal data takes place only in accordance with the explicit consent condition, the relevant person's withdrawal of the explicit consent,
- In accordance with article 11[1] of the PDPL, acceptance of the application for deletion and destruction of personal data within the framework of the rights of the person concerned is accepted by the Personal Data Protection Authority.

[1] **Related person's rights**
ARTICLE-11 (1) Everyone, by contacting the data controller about him/herself
a) Finding out if personal data is processed,
b) Requesting information if personal data has been processed,
c) Learning the purpose of processing personal data and whether they are used for their purpose,
ç) Knowing the third parties to whom personal data are transferred in Turkey or abroad,
d) Requesting correction of personal data if it is incomplete or incorrectly processed,
e) Request the deletion or destruction of personal data within the framework of the conditions stipulated in Article 7,

- In cases where the PDP Authority rejects the application made by the relevant person for the request of the deletion, destruction or anonymization of his personal data, he finds the answer he / she gave is insufficient or does not respond within the period stipulated in the PDPL, complain to the PDP Authority and this request is approved by the PDP Authority,
- That maximum time has passed that requires the storage of personal data and no condition exists to justify storing personal data for a longer period of time.,

is deleted by our association upon the request of the person concerned, destructed or deleted manually, destructed or anonymized.

6. TECHNICAL AND ADMINISTRATIVE MEASURES

For the purpose of storing your personal data safely, processing illegally, preventing access and destroying the data in accordance with the law, all administrative and technical measures taken by Global Communities within the framework of the principles in article 12 of the PDPL and in the Personal Data Security Guide published by the PDP Institution are listed below:

TECHNICAL MEASURES

The technical measures taken by our association regarding the personal data it processes are listed below:

- With penetration tests, necessary measures are taken by revealing the risks, threats, weaknesses and openings, if any, for the information systems of our Institution.
- As a result of real-time analysis with information security incident management, risks and threats that will affect the continuity of information systems are constantly monitored.
- Access to information systems and authorization of users is done through security policies over the access and authority matrix and the corporate active directory.
- Necessary precautions are taken for the physical security of the information systems equipment, software and data of the institution.
- To ensure information systems security against environmental threats, precautions for hardware (access control system that allows only authorized personnel to enter the system room, 24/7 monitoring system, ensuring the physical security of the side switches that make up the local area network, fire extinguishing system, air conditioning system etc.) and software (firewalls, attack prevention systems, network access control, systems that prevent harmful software, etc.).
- Risks to prevent illegal processing of personal data are identified, technical measures are taken to ensure compliance with these risks, and technical controls are made for the measures taken.

f) Requesting notification of transactions made in accordance with subparagraphs (d) and (e) to third parties to whom personal data are transferred,
g) Objection to the emergence of a result against the person by analyzing the processed data exclusively through automated systems,
ğ) Request the removal of the damage in case the personal data is damaged due to illegal processing of the data.

- By establishing access procedures within the institution, reporting and analysis studies on access to personal data are carried out.
- Access to storage areas with personal data is recorded and improper access or access attempts are kept under control.
- The institution takes the necessary measures to make the deleted personal data inaccessible and reusable for the relevant users.
- In case personal data are obtained illegally by others, an appropriate system and infrastructure have been established by the Authority to report this to the relevant person and the Board.
- Appropriate security patches are installed by following security gaps and information systems are kept up to date.
- Strong passwords are used in electronic environments where personal data are processed.
- Secure recording (logging) systems are used in electronic environments where personal data are processed.
- Data backup programs are used, which ensure the safe storage of personal data.
- Access to personal data stored in electronic or non-electronic environments is restricted according to access principles.
- The institution is encrypted with SHA 256 Bit RSA algorithm by using secure protocol (HTTPS) to access the website.
- A separate policy has been determined for the security of personal data with special features.
- Special training on personal data security was given to employees involved in special personal data processing processes, confidentiality agreements were made, and the powers of users who have access to data were defined.
- Special training on personal data security was given to employees involved in special personal data processing processes, confidentiality agreements were made, and the powers of users who have access to data were defined.
- Adequate security measures are taken in physical environments where special personal data are processed, stored and / or accessed, and unauthorized entry and exit are prevented by ensuring physical security.
- If special quality personal data should be transferred via e-mail, it is transmitted in encrypted form via corporate e-mail address or using KEP account. If it needs to be transferred via media such as portable memory, CD, DVD, it is encrypted with cryptographic methods and the cryptographic key is kept in different media. If the transfer is made between servers in different physical environments, data transfer is performed by installing VPN between servers or by sFTP method. If it is required to be transported through the paper medium, necessary measures are taken against the risks such as stolen, lost or seen by unauthorized people and the document is sent in “confidential” format.

ADMINISTRATIVE MEASURES

The administrative measures taken by the institution regarding the personal data it processes are listed below:

- In order to improve the quality of employees, trainings are provided on the prevention of illegal processing of personal data, prevention of unlawful access of personal data, protection of personal data, communication techniques, technical knowledge skills, Law No. 657 and other relevant legislation.
- Confidentiality agreements are signed for employees regarding the activities carried out by the Authority.
- The disciplinary procedure to be implemented for employees who do not comply with the security policies and procedures has been prepared.
- Before starting to process personal data, the Authority fulfills its obligation to enlighten the relevant persons.
- Personal data processing inventory was prepared.
- Periodic and random audits are carried out in-house.
- Information security trainings are provided for employees.

7. PERSONAL DATA DESTRUCTION TECHNIQUES

7.1. Deletion of Personal Data

Although our association has been processed in accordance with the provisions of the relevant law, in case the reasons requiring its processing disappear, it may delete personal data based on its own decision or upon the request of the personal data owner. Deletion of personal data is the process of making personal data inaccessible and unusable for the users concerned. Our association takes all necessary technical and administrative measures to make the deleted personal data inaccessible and reusable for the users concerned.

Personal Data Deletion Process

The process to be followed in the deletion of personal data is as follows:

- Identification of personal data that will be the subject of deletion.
- Identify relevant users for each personal data using the access authorization and control matrix or similar system.
- Determination of the authorities and methods of the relevant users such as access, retrieval and reuse.
- The closure and elimination of access, retrieval, reuse powers and methods of the relevant users within the scope of personal data.

Methods of Deleting Personal Data

Data Recording Environment	**Explanation**
Personal Data on Servers	For those who expire the time that requires the storage of personal data on the servers, the system administrator can remove the access authorization and delete it.

Personal Data in Electronic Environment	Those who expire that require the storage of personal data in the electronic environment are made inaccessible and unusable for other employees (related users) except for the database manager.
Personal Data in Physical Environment	For those who expire to be kept from the personal data kept in physical environment, it is made inaccessible and unusable for other employees except for the unit manager responsible for the document archive. In addition, blackening process is applied by drawing / painting / erasing in an unreadable manner.
Personal Data on Portable Media	Those that expire that require the storage of personal data held in flash-based storage media are stored in secure environments with encryption keys by encrypting them by the system administrator and granting access authority only to the system administrator.

Since personal data can be stored in various recording media, they should be deleted with methods appropriate for recording media. Examples of this are listed below:

- Application Type as a Service Cloud Solutions (such as Office 365 Salesforce, Dropbox): Data should be deleted by giving a delete command in the cloud system. It should be noted that while the aforementioned process is being carried out, the relevant user does not have the right to restore deleted data on the cloud system.
- Personal Data on Paper Media: Personal data on paper media should be deleted using the blackout method. Blackening process is done by cutting the personal data on the relevant documents whenever possible, and making it invisible to the relevant users by using fixed ink, in cases where it is not possible to be returned and cannot be read with technological solutions.
- Office Files on the Central Server: The file should be deleted with the delete command in the operating system or the access rights of the relevant user should be removed on the directory where the file or file is located. It should be noted that the user concerned is not a system administrator at the same time.
- Personal Data in Portable Media: Personal data in Flash based storage media should be stored in encrypted form and deleted using software suitable for these media.
- Databases: The relevant lines containing personal data should be deleted with database commands (DELETE etc.). It should be noted that the user concerned is not a database administrator at the same time.

7.2. Destruction of Personal Data

Although our association has been processed in accordance with the provisions of the relevant law, in case the reasons requiring its processing disappear, it may destroy personal data based on its decision or upon the request of the personal data owner. The destruction of personal data is the process of making

personal data inaccessible, irreversible and reusable by anyone. The data controller is responsible for taking all necessary technical and administrative measures regarding the destruction of personal data.

Data Recording	Explanation
Personal Data in Physical Environment	Those who expire to be stored from the personal data contained in the paper environment are irreversibly destroyed in paper clipping machines.
Personal Data in Optical / Magnetic Media	Physical destruction, such as melting, burning or powdering of those that expire, which requires storage from personal data contained in optical media and magnetic media, is applied. In addition, the magnetic media is passed through a special device and exposed to a high value magnetic field, making the data on it unreadable.

- Physical Destruction: Personal data can also be processed in non-automatic ways, provided that it is part of any data recording system. While erasing / destroying such data, the system of physical destruction of personal data, which cannot be used later, is implemented.
- Safely Deleting from Software: While deleting / destructing data that is processed in completely or partially automated ways and stored in digital media, methods for erasing the data from the related software are used in a way that cannot be recovered again.
- Securely Delete by Expert: In some cases, he may agree with a specialist to delete personal data on his behalf. In this case, the personal data is securely deleted / destrcuted by the person skilled in the art, so that it cannot be recovered again.
- Blackening: It is to make personal data physically unreadable.

Personal Data Destruction Methods

In order to destruct personal data, it is necessary to detect all copies of the data and to destroy them one by one of the following methods depending on the type of systems where the data is located:

- Local Systems: One or more of the following methods can be used to destroy data on said systems. i) De-magnetizing: It is the process of exposure of the magnetic media through a special device to an unreasonably corrupt data by exposing it to a high value magnetic field. ii) Physical Destruction: It is the process of physical destruction such as melting, burning or powdering of optical media and magnetic media. Data is rendered inaccessible by processes such as melting, burning, powdering or passing through a metal grinder. If the process of overwriting or de-magnetizing in terms of solid state discs is not successful, this media must also be physically destroyed. iii) Overwrite: It is the process of preventing the recovery of old data by writing random data consisting of 0 and 1 at least seven times on magnetic media and rewritable optical media. This process is done using special software.

- Environmental Systems: The disposal methods that can be used depending on the media type are as follows: İ) Network devices (switch, router etc.): The storage media in the said devices are fixed. Products often have a delete command, but do not destroy. The appropriate methods

specified in (a) must be destroyed by using one or more of them. ii) Flash based environments: Flash based hard drives with ATA (SATA, PATA etc.), SCSI (SCSI Express etc.) interface should be destructed by using the <block erase> command if supported, if not, byusing the manufacturer's proposed destruction method, or using one or more of the appropriate methods specified in (a). iii) Magnetic tape: These are the media that store the data with the help of micro magnet pieces on the flexible tape. It must be destroyed by exposing it to very strong magnetic environments and de-magnetizing or by physical destruction methods such as burning and melting. iv) Units such as magnetic disc: These are the media that store the data with the help of micro magnet pieces on flexible (plate) or fixed media. It must be destroyed by exposing it to very strong magnetic environments and de-magnetizing or by physical destruction methods such as burning and melting. v) Mobile phones (Sim card and fixed memory areas): There is a delete command in the fixed memory areas of portable smart phones, but most of them do not have a destruction command. The appropriate methods specified in (a) must be destroyed by using one or more of them. vi) Optical discs: Data storage media such as CDs and DVDs. It must be destructed by physical destruction methods such as burning, chopping, melting. vii) Peripherals such as printer, fingerprint door access system that can be removed from the data recording medium: It should be destroyed by using one or more of the appropriate methods specified in (a), verifying that all data recording media are removed. viii) Peripherals such as printer with fixed data recording environment, fingerprint door access system: Most of these systems have a delete command, but no destruction command. The appropriate methods specified in (a) must be destroyed by using one or more of them.

- Paper and Microfiche Environments: Since the personal data in these media are permanently and physically written on the media, the main media must be destroyed. While this process is being carried out, it is necessary to divide the media into small pieces in an incomprehensible size, if possible horizontally and vertically, not to be combined back together with paper disposal or clipping machines. Personal data transferred from the original paper format to electronic media by scanning should be destroyed by using one or more of the appropriate methods specified in (a) according to the electronic environment in which they are located.

- Cloud Environment: During the storage and use of the personal data contained in the said systems, encryption keys must be used separately for cryptographic methods and where possible for personal data, especially for each cloud solution where the service is received. When the cloud computing service relationship ends, all copies of the encryption keys required to make personal data available must be destroyed. In addition to the above environments, the process of destroying personal data in devices that are malfunctioning or sent for maintenance is carried out as follows: i) The destruction of the personal data contained in (a) by using one or more of the appropriate methods specified in (a) before transferring it to third institutions such as manufacturer, seller, service for maintenance, repair, ii) In cases where destruction is not possible or appropriate, storing the data storage medium and sending other defective parts to third institutions such as manufacturer, seller service, iii) Necessary precautions must be taken to prevent the personnel coming from outside for maintenance, repair, etc. from copying the personal data out of the institution.

7.3. Anonymization of Personal Data

Anonymization of personal data implies that personal data cannot be associated with an identified or identifiable natural person by any means, even by matching with other data. Our association can anonymize personal data when the reasons that require the processing of personal data processed in accordance with the law are eliminated. In order for personal data to be anonymized, personal data should be rendered unrelated to a specific or identifiable natural person, even by using appropriate techniques for the recording environment and the relevant field of activity, such as returning data by the data controller or recipient groups and / or matching the data with other data. Our association takes all necessary technical and administrative measures to anonymize personal data.

Personal data anonymized in accordance with Article 28 of the PDPL can be processed for purposes such as research, planning and statistics. Such transactions are outside the scope of the PDPL and the explicit consent of the personal data owner will not be sought.

Anonymization Methods of Personal Data

Anonymization of personal data is to make personal data unrelated to an identified or identifiable natural person by any means, even if it is matched with other data.

In order for personal data to be anonymized, personal data should be rendered unrelated to a specific or identifiable natural person, even by the use of appropriate techniques for the recording environment and related field of activity, such as returning data by the data controller or third parties and / or matching the data with other data.

Anonymization means that by removing or changing all direct and / or indirect identifiers in a data set, the identity of the person concerned is prevented from being detected, or loses its distinction in a group or crowd that cannot be associated with a natural person. Data that does not indicate a specific person as a result of blocking or loss of these features is considered anonymized data. In other words, the anonymized data is the information that identifies a real person before this process, while it became unrelated to the relevant person after this process and the connection with the person was broken. The purpose of anonymizing is to break the link between the data and the person that this data describes. All processes of disconnection carried out by methods such as automatic or non-grouping, masking, derivation, generalization, randomization applied to records in the data recording system where personal data is kept are called anonymization methods. The data obtained as a result of applying these methods should not be able to identify a particular person.

Anonymization methods that can be sampled are described below:

Anonymization Methods That Do Not Provide Value Irregularity: In methods that do not provide value irregularity, no changes or additions or subtractions are applied to the values owned by the data in the cluster, instead, changes are made to the rows or columns in the cluster. Thus, while the data changes throughout the data, the values in the fields maintain their original state.

a. Extracting Variables

It is a method of anonymization provided by deleting one or more of the variables from the table completely. In this case, the entire column in the table will be completely removed. This method can

be used for reasons such as the variable being a high-level descriptor, the lack of a more appropriate solution, the variable being too sensitive to be disclosed to the public or not serving analytical purposes.

b. Extracting Records

In this method, anonymity is strengthened by removing a line containing singularity in the dataset and the possibility of making assumptions about the dataset is reduced. Generally, the records that are issued are records that do not have a common value with other records and people who have an idea about the data set can easily guess. For example, in a dataset with survey results, only one person from any industry is included in the survey. In such a case, it may be preferable to remove only the record belonging to this person, rather than subtracting the “sector” variable from all survey results.

c. Regional Hiding

In the regional hiding method, the aim is to make the dataset more secure and reduce the risk of predictability. If the combination created by the values of a particular record creates a very visible situation and this situation may cause that person to become discernible in the relevant community, the value that creates the exceptional situation is changed to "unknown".

ç. Generalization

It is the process of converting related personal data from a special value to a more general value. It is the most used method in generating cumulative reports and in operations carried out on total figures. The resulting new values show the total values or statistics for a group that makes it impossible to access a real person. For example, a person with a Turkish Identity Number 12345678901 has received a wet wipe after buying diapers from the e-commerce platform. By using the generalization method in the anonymization process, it can be concluded that xx% of people who buy diapers from the e-commerce platform are also buying wet wipes.

d. Lower and Upper Limit Coding

The upper and lower limit coding method is obtained by defining a category for a given variable by combining the remaining values in the grouping created by this category. Generally, the low or high values of the values in a certain variable are gathered together and a new definition is made for these values.

e. Global Coding

Global coding method is a grouping method used in datasets with lower and upper limit coding that cannot be applied, do not contain numerical values or have numerical values. Generally, it is used when certain values are clustered, making it easier to carry out forecasts and assumptions. By creating a common and new group for the selected values, all records in the data set are replaced with this new definition.

f. Sampling

In the sampling method, instead of the whole data set, a subset from the set is explained or shared. Thus, since it is not known whether a person known to be in the whole data set is included in the described or shared sample subset, the risk of generating accurate predictions about individuals is reduced. Simple statistical methods are used to determine the subset to be sampled. For example, if the demographic information, occupations and health status of women living in Istanbul are anonymized or shared, it can be meaningful to make scans and make predictions about a woman who

is known to live in Istanbul. However, in the data set, only the women whose province is Istanbul, are registered and anonymization is applied by removing the population record from other provinces and if the data is disclosed or shared, because of the fact that the malicious person who accesses the data cannot estimate whether the population record of a woman she knows lives in Istanbul, he/she will not be able to make a reliable estimate of whether the information that he/she knows is contained in the data of this person.

Anonymization Methods That Provide Value Irregularity: Unlike the methods mentioned above with the methods that provide value irregularity, the existing values are changed and the values of the data set are damaged. In this case, since the values carried by the records are changing, the benefit planned to be obtained from the data set should be calculated correctly. Even if the values in the dataset are changing, it is possible to continue to benefit from the data by ensuring that the total statistics are not disrupted.

Micro Merge

With this method, all the records in the dataset are first sorted in a meaningful order and then the whole set is divided into a certain number of subsets. Then, by taking the average of the value of each subset of the specified variable, the value of that variable of the subset is replaced with the average value. Thus, the average value of that variable valid for the whole data set will not change.

Data Exchange

The data exchange method is the record changes obtained by exchanging the values of a variable subset between the couples selected from the records. This method is mainly used for variables that can be categorized and the main idea is to transform the database by changing the values of the variables between the individual records.

Add Noise

With this method, additions and subtractions are performed to provide the distortions in a selected variable to the specified extent. This method is mostly applied in datasets containing numerical values. Distortion is applied equally at every value.

Statistical Methods to Strengthen Anonymization

As a result of combining some values in the anonymized datasets with individual scenarios, the possibility of identifying the individuals in the records or deriving assumptions about their personal data may arise.

For this reason, anonymity can be strengthened by minimizing the uniqueness of records in the data set by using various statistical methods in anonymized datasets. The main purpose in these methods is to minimize the risk of anonymity deterioration while keeping the benefit to be obtained from the dataset at a certain level.

a. K-Anonymity

In anonymized datasets, if indirect identifiers come together with the correct combinations, the identification of the persons in the records or the predictability of information about a particular person has shaken the confidence in the anonymization processes. Accordingly, data sets that were anonymized with various statistical methods had to be made more reliable. K-anonymity has been developed to ensure that more than one person is identified with specific fields in a data set, preventing the disclosure of personal information that shows individual characteristics in certain combinations. If there are more than one record of combinations created by combining some of the

variables in a dataset, the probability of identifying the persons corresponding to this combination can be reduced.

b. L- Multiplicity

The L-diversity method, which is formed by studies carried out on the deficiencies of K-anonymity, takes into account the diversity formed by sensitive variables corresponding to the same variable combinations.

c. T-Proximity

Although the L-diversity method provides diversity in personal data, there are occasions when the method in question cannot provide adequate protection as it is not concerned with the content and degree of sensitivity of the personal data. In this way, the process of calculating the degree of closeness of personal data and values within each other and anonymizing the data set according to these proximity levels is called T-proximity method.

Selecting Anonymization Method

Our association decides which of the above methods will be applied by looking at the data they have and considering the following features regarding the data set owned;

- The nature of the data,
- The size of the data,
- The structure of data in physical environments,
- The diversity of the data,
- Benefit from the data / purpose of processing,
- Data processing frequency,
- Reliability of the party to whom the data will be transferred,
- The effort to make the data anonymous is meaningful,
- The magnitude of the damage that can occur if the anonymity of the data is impaired, the area of influence,
- The distribution / centrality ratio of the data,
- Users' authority control of access to relevant data; and
- The probability that his effort to construct and implement an attack that would disrupt anonymity would be meaningful.

While anonymizing a data, our Association checks whether the data in question re-identifies a person through the contracts and risk analyzes it will make using the information known to be within the body of other institutions and organizations.

Anonymity Assurance

While our association decides to anonymize a personal data rather than being deleted or destroyed, it wishes to consider the anonymity of the anonymized dataset by combining it with a thousand other datasets, the fact that a thousand or more than one value is not created in a way that makes a record singular, the values in the anonymized dataset are combined and cannot produce an assumption or result, and as our association anonymizes, the checks are made as the features listed in this article change and it is ensured that anonymity is maintained.

Risks of Disrupting Anonymization by Reverse Processing of Anonymized Data

Since the anonymization process is the process of destroying the distinctive and identifying features of the data set and applied to personal data, there is a risk that these processes will be reversed with various interventions and that the anonymized data will become re-identifying and real people distinctive. This situation is expressed as the disruption of anonymity. Anonymization operations can only be achieved by manual or automatic enhanced processes, or by hybrid processes that are a combination of both types of processes. However, the important thing is that after the anonymized data has been shared or disclosed, measures have been taken to prevent anonymity deterioration by new users who can access or own the data. The deliberate processes of anonymity deterioration are called “attacks on anonymity deterioration”. In this context, our Association investigates whether there is a risk of reversing anonymized personal data with various interventions and turning anonymized data back into identifying and distinctive people.

8. PERSONNEL

All units and employees of the association actively support responsible units for taking technical and administrative measures to ensure data security in all environments where personal data is processed in order to ensure the proper implementation of the technical and administrative measures taken by the responsible units within the scope of the Policy, to increase the training and awareness of the unit employees, to monitor and constantly control them, to prevent the illegal processing of personal data, to prevent the unlawful access to personal data and to ensure that the personal data are kept in accordance with the law.

You can access the titles, units and job descriptions of the personnel involved in the process of personal data retention and destruction from the table in ANNEX-1 of this Policy.

9. RETENTION AND DESTRCUTION PERIODS

Regarding the personal data processed by our association within the scope of its activities;

- Retention periods based on personal data related to all personal data within the scope of activities carried out depending on the processes are included in the Personal Data Processing Inventory.;
- Retention periods based on data categories are included in VERBİS.
- Process-based retention periods are included in the Personal Data Retention and Destruction Policy.

If necessary, updates are made by the Turkey office internal PDP committee on these retention periods. For personal data whose retention periods have expired, the deletion, destruction or anonymization process is carried out by the focal point of each department / unit.

You can reach the table showing the retention, destruction and periodic destruction periods of your personal data obtained by our Association in accordance with the provisions of PDPL and other relevant legislation, from the “Retention and Destruction Period Table” in Annex-2 of this Policy.

In addition to the destruction periods included in Appendix-2 of this Policy, Global Communities destroy personal data in 6 month periods in accordance with the procedures contained in this Policy,

which expires on a monthly basis. Accordingly, the Association carries out periodic annihilation every year in January and June.

All transactions regarding the deletion, destruction and anonymization of personal data are recorded and these records are kept for at least three years, excluding other legal obligations.

10. OTHER ISSUES

In case of inconsistency between PDPL and other relevant legislative provisions and this Policy, firstly, PDPL and other relevant legislative provisions will be applied. The printed copy of this Policy is kept by the Administration department.

This Policy prepared by the Global Communities came into force on 29.12.2020 following the decision of the Board of Directors of the Association. In case of changes in the Policy, the effective date of the Policy and the related articles will be updated accordingly. The update table is included in Annex-3.

If it is decided to repeal the policy, the old copies of the policy with a wet signature are canceled by the Administration department (with the cancellation stamp or a cancellation) by the decision of the Board of Directors and kept by the Administration department for a minimum of 5 years.

Any question regarding this policy can be directed to PDP Internal Committee.

Global Communities Inc. Turkey Representatıve Office

ANNEX-1 PERSONNEL TITLE, UNIT AND DUTY LIST

TITLE	**UNIT**	**DUTY**
Senior Admin Officer	Administration	Responsible for personal data retention and destruction of administration department, keeping minutes of destruction document of administration department. Keeping other departments' originals of minutes of destruction document.
Office Manager	Administration	Responsible for personal data retention and destruction of administration department, ensuring minutes of destruction document of administration is kept and secured well.
IT Coordinator	IT	Responsible for personal data retention and destruction of IT department. Keeping minutes of destruction document of IT department
Senior Operations Manager	Operations	Responsible for personal data retention and destruction of operations department (Procurement and Logistics), ensuring minutes of destruction document of Operations is kept and secured well.
Senior Procurement Officer	Operations	Responsible for personal data retention and destruction of Procurement department, keeping minutes of destruction document of procurement department
Senior Operations Officer	Operations	Responsible for personal data retention and destruction of Logistics department, keeping minutes of destruction document of Logistics department
Senior HR Manager	HR	Responsible for personal data retention and destruction of HR department, keeping minutes of destruction document of HR department
Senior Security Analyst	Security	Responsible for personal data retention and destruction of administration department, keeping minutes of destruction document of Security department
Compliance Coordinator	Compliance	Responsible for personal data retention and destruction of administration department, keeping minutes of destruction document of Compliance department
Senior Finance Officer	Finance	Responsible for personal data retention and destruction of administration department, keeping minutes of destruction document of Finance department

ANNEX -2 TABLE OF RETENTION AND DESTRCUTION PERIODS

EK-2 SAKLAMA VE İMHA SÜRELERİ TABLOSU

Procedure	**Period**	**Expalanation**
CV, application form, all forms and technical tests during interview period	- 3 years - 10 years	- The curriculum vitae, job application forms, all forms in the interview process and technical test application dates of the candidates whose job applications are evaluated positively / negatively and whose recruitment is not decided are kept for three years starting from the date of application and destroyed during the first periodic destruction process at the end of 3 years. - The curriculum vitae, job application forms, all forms in the interview process and technical test of the employed employees are destroyed in the first periodic destruction period after 10 years from the end of the employment contract of the employee.
Resedence card (conditional)	- 3 years - 10 years	- The curriculum vitae, job application forms, all forms in the interview process and technical test application dates of the candidates whose job applications are evaluated positively / negatively and whose recruitment is not decided are kept for three years starting from the date of application and destroyed during the first periodic destruction process at the end of 3 years. - The curriculum vitae, job application forms, all forms in the interview process and technical test of the employed employees are destroyed in the first periodic destruction period after 10 years from the end of the employment contract of the employee.
Documents in the recruitment process for selected candidates (Identity, Bio data form,	- 3 years - 10 years	If the employment contract is signed with the employee candidate who is planned to be employed, it is kept for 10 years from the termination of the employment contract, but if the contract is not signed, it is destroyed

General release form , Training certificate, possible conflict of interest declaration form, References, OFAC check, security review, salary verification, recruitment document, offer form)		in the first periodic destruction process at the end of 3 years.
All documents in the employee personnel file (identity / passport, CV, GC personnel data form, GC confidentiality agreement, Code of Conduct acceptance documents, bank account information, photograph, criminal record documents, Family information, Residence information, Health check for work, Orientation form, Employment contract, SSI registration / cancellation, Podio registration, Timesheet system records, Safety registration / cancellation, possible conflict of interest declaration form, Employee information form, welcome notice,	- 10 years	It is kept for 10 years from the termination of the employment contract signed with the employee and destroyed in the first periodic destruction process.

acceptance statement notes for documents, Trial Period evaluation forms, additions / regulations to contracts, Employee guide Declaration of acceptance, Half-year and Year-end performance evaluation forms, Warning letters, Training / workshop etc. correspondence, working time and leave records, payroll, resignation letter, resignation acceptance letter, employment termination documents, employment certificate, Human resources documents and notes and other documents containing personal data)		
Inventory	- 10 years - 15 years	It is kept for 10 years from the termination of the employment contract signed with the employee and destroyed in the first periodic destruction process. Protective equipment debit documents that are embezzled within the scope of work security are kept for 15 years following the working process.
Travel/Accomodation Documents	- 10 Years	The information within the scope of travel and reservation (personnel data) should be kept until the relevant travel is completed and then deleted / destroyed. However, the period for keeping the financial records and documents related to travel and reservations in accordance with the accounting procedures is 10 years following the relevant tax year

		and the documents should be kept for 10 years following the tax year in which the documents are accounted.
ID/Business Card	Immediately	It is destroyed on the date the employee leaves the job.
The books, signature circulars, statutes, information and documents related to the establishment, etc.	- 5 years	The books, statutes, etc. regarding the establishment. The information and documents must be kept during the activity of the organization (foreign association, foundation or non-profit organization) and for a period of 5 years from the date of termination and liquidation.
Copy of work permit information / document and work permit cards	- 10 years	It is kept for 10 years from the termination of the employment contract signed with the employee and destroyed in the first periodic destruction process.
Organization / Training preparation and permission documents	- 5 years	It must be kept for 5 years during the activity of the organization (foreign association, foundation or non-profit organization) and from the date of its liquidation.
Work Safety and Security Documents/Files	- 15 years	OHS documents should be kept during the work of the relevant personnel and for a period of 15 years following their departure.
Lease Agreements	- 5 years	The relevant contract, information and documents must be kept for 5 years following the continuation and termination of the lease.
Protocol Documents	- 5 years	It must be kept for 5 years during the activity of the organization (foreign association, foundation or non-profit organization) and from the date of its liquidation.
Tax documents of third parties	- 10 years	It is kept as long as the commercial relationship with the relevant third parties continues and for 10 years following its termination.
Cvs of technical staff who works with vendor	5 years	It is destroyed during the first periodic destruction period following the expiry of the storage period.
Full Back ups on Cloud and NAS	Monthly	It is destroyed during the first periodic destruction period following the expiry of the storage period.
Incremental Back up – Bulut ve NAS	Daily	It is destroyed during the first periodic destruction period following the expiry of the storage period.
Execution of Hardware and Software Access Processes	2 years	It is destroyed during the first periodic destruction period following the expiry of the storage period.

Visitor and Attendees to workshops/meetings	2 years following the end of the event and the date of the visit	It is destroyed during the first periodic destruction period following the expiry of the storage period.
Contractual Relations	- 10 years	It is destroyed during the first periodic destruction period following the expiry of the storage period.
CCTV Records	- 30 days	It is destroyed during the first periodic destruction period following the expiry of the storage period.
Beneficiary Personal information, ID copies, Registration and distribution information for assistance.	- 3 years	It is destroyed during the first periodic destruction period following the expiry of the storage period.

ANNEX -3 UPDATE TABLE

This Policy was updated on [•]. Relevant changes consist of [•].