Personal Data Protection Policy

Table of Contents

As Global Communities Inc. Turkey Representative Office (Global Communities), we care about the privacy and security of your personal data. In this context, we would like to inform you about how we process the personal data we receive from our donors, volunteers, those in need, immigrants, suppliers, business partners, their employees and officials and all other third parties while conducting our activities. We would like to inform you about the purposes for which we use this data and how we protect this information.

All the concepts and expressions used in this notification will express the meaning attributed to them in Personal Data Protection Law No. 6698 (“KVKK” [Personal Data Protection Law - **PDPL**]) and other legislation. The expression "you" in this Statement refers to "you" personally. The term personal data is used to include special personal data.
The meanings expressed by the terms and abbreviations in this policy are included in the ANNEX - Abbreviations section.

We would like to remind you that if you do not accept the policy, you should not pass on your personal data. If you choose not to transmit your personal data to us, in some cases, we will not be able to provide you with our services, answer your requests, or ensure the full functionality of our services.

We would like to remind you that it is your responsibility to ensure that the personal data you transmit to our association are as accurate, complete and up-to-date as you know. In addition, if you share other people's data with us, it will be your responsibility to collect such data in accordance with local legal requirements. In this case, it means that you have obtained all necessary permissions from the third party in question for us to collect, process, use, and disclose their information, and our Association cannot be held responsible in this regard.

ABOUT GLOBAL COMMUNITIES INC. TURKEY REPRESENTATIVE OFFICE

Global Communities Inc. Turkey Representative office is registered to Association Desk of Turkey Ministry Of Interior since 2014, the organization is active and located in Gaziantep under Turkish law. All this year, the organization has reached a growing number of vulnerable people by implementing projects and activities.

The terms "we" or "Association" or "Global Communities" in the Policy, relates to personal data processing activities carried out by the Gaziantep Provincial Directorate of Associations as a Data Officer by the Global Communities Inc. Turkey Representative Office ("**Global Communities**") registered with the registration number US-27-001-097 and located at 15 Temmuz mah. 148031 nolu sok. No:3 A ve B Blok, Şehitkamil/Gaziantep/Turkey.

OUR PRINCIPLES OF PROCESSING PERSONAL DATA

All personal data processed by our association are processed in accordance with PDPL and related legislation. The basic principles and principles we consider when processing your personal data in accordance with article 4 of PDPL are explained below:

- **Processing in accordance with Law and the Integrity Rule**: Our association acts in accordance with the principles of legal regulations and general trust and honesty in the processing of personal

data. In this context, our Association takes into consideration the proportionality requirements in the processing of personal data and does not use personal data outside the purpose.

- **Ensuring that Personal Data are correct and Up-to-Date, as required**: Our association ensures that the personal data it processes are accurate and up-to-date, taking into account the fundamental rights of the personal data owners and their legitimate interests.
- **Processing for Specific, Clear and Legitimate Purpose**s: Our association determines the purpose of legitimate and lawful personal data processing clearly and precisely. Our association is connected with the products and services that it offers and processes as much as necessary for them.
- **Being Connected, Limited, and Metered for the Purpose they are processed** for: Our association processes the personal data in a convenient way to achieve the specified goals. And our association avoids processing personal data that are not related to the realization of the purpose or not needed.
- **Retaining for the Time required for the Purpose or Processed in the Relevant Legislation**: Our association maintains personal data only for the time required by the relevant legislation or for the purpose for which it was processed. In this context, our Association determines firstly whether a period is foreseen in the relevant legislation for the storage of personal data. If a period is determined, the association acts in accordance with this period, and if no period is determined, it stores the personal data for the time required for the purpose for which they are processed. In case the reasons that require the expiration or processing of the period disappear, personal data are deleted, destroyed or anonymized by our Association.

DATA OWNER CATEGORIES

The categories of data owners other than employees (including trainees and subcontractor employees) whose personal data are processed by our association are given in the table below. A separate policy regarding the processing of personal data of our employees has been established and implemented within the Association. People outside the categories below may also submit their requests to our Association within the scope of PDPL. Their demands will also be evaluated.

RELATED PERSON CATEGORY	DESCRIPTION
Donor / Volunteer	Real and legal entities that receive donations in cash or in kind or donate to realize the operational objectives of Global Communities and real persons working together with Global Communities to carry out activities without any economic interest while carrying out Global Communities activities.
Beneficiary	Natural persons to whom Global Communities provide assistance within their activities
Researcher	Real persons who benefit from the Global Communities archives
Potential Donor / Volunteer	Real or legal persons who have requested or are interested in cash and in-kind donations and / or donations or have been evaluated in accordance with the rules of honesty and integrity that they may have and real persons who have requested or have been interested in or engaged in activities with Global Communities to carry out activities without economic interest while conducting Global Communities activities.
Visitor	Real persons who have entered the physical facilities (offices etc.) owned by our association or organized an organization for various purposes or visit our websites.
Third Person (Party)	Third party natural persons who are associated with these individuals in order to ensure the security of the transaction between our parties mentioned above or to protect the rights and interests of those individuals.

	(Example: Guarantor, companion, family members and relatives) or all natural persons that our Association has to process personal data for a specific purpose, even if it is not explicitly stated in the Policy (Example: former employees)
Employee Candidate / Trainee Candidate	Real persons who have applied to our association in any way, or who have opened their CV and related information for our Association's review.
Global Communities Economic Enterprise Employee	Employees and representatives of the economic enterprises established by our association in order to achieve their operational objectives.
Employees, Shareholders, Authorities of Institutions We Are In Cooperation With	Real persons, including shareholders and officials of those institutions working in institutions (business partners, suppliers, etc., but not limited to) that our association has any kind of relationship with.

WHEN DO WE COLLECT PERSONAL DATA ABOUT YOU?

We basically collect your personal data in the following situations:

- When you are a Donor or volunteer of Global Communities,
- When you take advantage of the services offered by Global Communities
- When you access the Global Communities archives
- When you participate in camps organized by Global Communities
- When you sell goods or provide services to us,
- When you subscribe to our newsletters and choose to receive our messages,
- When you contact us to send complaints or feedback via e-mail or telephone,
- When you apply for a job to our association,
- When you join our association events, seminars, conferences and organizations,
- When you contact us for any purpose as a potential donor / volunteer / supplier / partner / subcontractor.

We will only process the personal data we have obtained in the above cases in accordance with this Policy.

What personal data do we process about you?

The personal data we process about you depends on the type of relationship we have between us (For example, donor, in-kind or cash donor, volunteer, needy, beneficiary, supplier, business partner, etc.) and this personal data varies according to how you contact us (For example, phone, e-mail, printed documents, donor consent form, stem cell donor consent form, etc.)

Basically, our personal data processing methods are situations in which you participate in our business events, surveys or interact with us in any other way, by phone or e-mail. In this context, the personal data we process can be explained under the following categories:

Data categories	**Examples**
ID information	Information contained in identity documents such as name, surname, title, date of birth, place of birth, TR identity number, identity card and passport photocopies, signature
Contact information	Email, phone number, address

Data categories	Examples
Pictures and / or videos that can identify you	Photo and video images and audio data processed when you visit our association for security reasons or when you attend events organized by our Association.
Financial data	Bank account data, billing information
Education information	School information, education status information, Certificate Information, graduation date
Any other information you decide to share voluntarily with Global Communities	Personal data that you share with your own initiative, feedback, opinions, requests and complaints you send to us, evaluations, comments and our evaluations about them, uploaded files, interests, information for our detailed review process before establishing a business relationship with you.
Electronic data collected automatically	When you visit or use our website or apps, subscribe to our newsletters, interact with us through other electronic channels, In addition to the information you transmit directly to us, we may also collect electronic data sent to us by your computer, mobile phone, or other access device. (Example: device hardware model, IP address, operating system version and settings, hours and duration of using our digital channel or product, your actual location, links you click, which can be collected when you activate location-based products or features, motion sensor data etc.)
Legal action and compliance information	Your personal data processed within the scope of determination of legal receivables and rights, follow-up and performance of our debts as well as our legal obligations and compliance with our Association's policies.
Health Information	
Information on Criminal Convictions and Security Measures	Criminal record
Supplier data	As a result of the operations carried out by our business units within the scope of our services, information obtained about the data owner, such as the data owner supplier or the data owner such as the employee and signature officer within the body of the supplier.
Incident management and security information	Information and evaluations collected about the events that have the potential to affect the employees or managers of our association, vehicle license plate and vehicle information, transportation and travel information.

Data categories	Examples
Personal data collected from other sources	To the extent permitted by applicable laws and regulations, we may also collect your personal data through publicly available databases, methods and platforms where our partners we work with collect personal data on our behalf. For example, we may investigate you to ensure the technical, administrative and legal security of our Association from public sources before establishing a relationship with you. In addition, it may be possible for you to transmit some personal data belonging to third parties by you. In order to manage our technical and administrative risks, we may process your personal data through methods used in accordance with the generally accepted legal, customary and honesty rules in these areas.

PROCESSING THE PERSONAL DATA OF EMPLOYEE CANDIDATES

In order to understand the candidate's experience and qualifications as well as the personal data categories listed above and to evaluate the suitability of the candidate for open position, to check the accuracy of the information conveyed if necessary and to conduct research about the candidate by contacting the third parties to whom the candidate's contact information is provided, to contact the candidate regarding the job application process, recruitment in accordance with the open position, to ensure compliance with legal regulations and we collect personal data of the school, previous work experience, disability, etc. that our Association graduated in order to apply recruitment rules and human resources policies.

Personal data of employee candidates, job application form available in written and electronic media, electronic job application platform of our Association, physical or e-mail applications to our Association, employment and consultancy associations, face-to-face or electronic interviews, Controls made by our association on the candidate for employment, The recruitment tests carried out by human resources experts to evaluate the suitability of the candidate during the recruitment process are processed through means.

Employee candidates are illuminated in detail in accordance with PDPL with a separate document before submitting their personal data when applying for a job and their express consent is obtained for the necessary personal data processing activities.

PROCESSING OF PERSONAL DATA OF OUR VISITORS IN OUR OFFICES

Our Association processes personal data for the purpose of controlling the workplace rules in order to ensure the physical security of our Association, our employees and visitors during the entrance and exit processes of the visitors coming to the building. In this context, the name - surname and TR identity numbers of our visitors are confirmed with their IDs and recorded in the visitors book for the purpose of visitor entrance and exit. However, the visitor's identity is not kept during his stay in the Association, and the identity is given back to the visitor after the mentioned registration is made in the guestbook.

Before the information is received, the visitor is illuminated regarding the processing of his personal data with an illumination text located at the security entrance. However, since our Association has a legitimate

interest in this context, the explicit consent of the visitor is not taken in accordance with PDPL article 5/2 / f. These data are only physically kept in the visitor logbook and are not transferred to another medium unless there is a doubtful situation that threatens the security of the Association. However, this information can be used in cases such as prevention of crime and ensuring the security of the association.

In addition to this, internet access can be provided to our requesting visitors during their stay in the offices of our Association for the purposes specified in the Policy and ensuring security by our Association. In this case, the log records related to your internet access are recorded according to the mandatory provisions of the Law No. 5651 and the legislation issued according to this law. These records are processed only to be requested by authorized public institutions and organizations, by the organization's policies for safety and security of the Association or to fulfill our legal obligations in the audit processes to be carried out within the Association.

Only a limited number of Global Communities employees are able to access the log records obtained within this framework. Employees of the Association, who have access to the aforementioned records, access these records only for use in the request or audit processes from the authorized public institution and organization. And the employees of the Association share this information with legally authorized persons.

PROCESSING PERSONAL DATA BY CLOSED CIRCUIT CAMERA RECORDING

Security cameras are used to ensure the safety of our association and personal data is processed in this way. Within the scope of monitoring activity with our security camera; It aims to increase the quality of the service provided, to ensure the safety of life and property of the physical campuses of the Association and the people in the Association, to prevent abuse, and to protect the legitimate interests of data owners.

Personal data processing activities conducted by our association with security cameras are carried out in accordance with the Constitution, PDPL and the relevant legislation.

In accordance with PDPL article 4, our association processes personal data in a connected, limited and measured manner for the purpose for which they are processed. It is not subjected to monitoring the privacy of the person as a result of intervention that exceeds security objectives. In this context, warning signs are placed in common areas where CCTV recording is made and data owners are informed. However, because of the legitimate interest of our Association in keeping CCTV records, their open consent is not obtained.

In addition, in accordance with PDPL article 12, necessary technical and administrative measures are taken to ensure the security of personal data obtained as a result of CCTV monitoring activity.

In addition, a procedure has been prepared for the areas with CCTV cameras, the viewing areas of the cameras, and the duration of the recording and application has been taken in our Association. This procedure is taken into consideration before the CCTV camera is installed and the camera is then placed. Camera placement is not allowed to exceed the security intent and the privacy of individuals. CCTV camera images are only accessed by a certain number of Association staff and these powers are regularly reviewed. Staff who have access to these records sign a commitment to protect personal data in a lawful manner.

The entrance doors, building exterior, visitor waiting hall, on stairs in entrance and exit in basement in our association offices are recorded with a total of 11 security cameras in the service area and in order to ensure the security of the building, the image is recorded and supervised by the Security and IT departments.

FOR WHAT PURPOSES DO WE USE YOUR PERSONAL DATA?

Our purposes of using your personal data depend on the type of business relationship between us. It varies according to (e.g. donor, volunteer, beneficiary, supplier, business partner, etc.) Basically, our purposes for processing your personal data are listed below. Personal data processing activities regarding the Candidates for Employees are explained under the section "Processing of Personal Data of Employee Candidates" above.

.

Our Personal Data Processing Purposes	**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, transferring donations to the system through activities and campaigns carried out by Global Communities (for both individual and corporate donors), receiving in-kind and cash donations, informing the candidate of the donor, determining the identity of the donor candidate, receiving donations, transmitting donations to required places, fulfilling requests of donors who want to update their credentials, control of payments, checking whether they are on the list of people who should not be taken specifically for the services and products received.
Establishment and management of beneficiary relations	Determining the needs and the needs of these people, Evaluation of request forms from Global Communities branches, Carrying out financial processes for the purpose of providing cash aids to those in need and making cash aids,
Execution and finalization of the contract process with our suppliers / business partners	Managing the supply and billing process of our association, purchasing services and materials, establishing and executing a contract, ensuring the legal transaction security after the contract, storing the information after the contract, filling the form after the purchase of goods, Taking the data of the people who bought the goods, developing service, evaluating new technologies and applications, and determining and implementing our Association's strategies, managing operations (demand, proposal, evaluation, order, budgeting, contract), evaluating processes within the scope of the organization in terms of compliance and minimizing risks, standard of behavior, training in processes related to compliance such as fraud, conducting investigations, control of financial operations and records, managing financial affairs, organizing tenders for outsourcing.
Conducting direct marketing processes	To make notifications regarding our activities by e-mail and telephone, conducting satisfaction surveys or social media, evaluation of your opinions, complaints and comments made through online platforms or other channels, returning, To inform the participants about the activities

Our Personal Data Processing Purposes	Examples
	of Global Communities 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	Execution of tax and insurance processes, Associations Law No. 5253, Law No. 5072 on the Relations of Associations and Foundations with Public Institutions and Organizations, Law 5651 and other legislation, Law on Regulation of Electronic Trade No. 6563 and other legislation, Turkish Penal Code No. 5237 Law No. 6698 on Protection of Personal Data, Fulfilling our legal obligations arising from the relevant legislation, execution of processes before official institutions, record keeping and information obligations, compliance and audit, audit and inspection of official authorities, following and finalizing our legal rights and cases, execution of the necessary processes within the scope of compliance with the laws and regulations we are subject to, such as disclosure of data at the request of the official authorities (Sharing information with the Ministry of Family and Social Policies in processes carried out regarding beneficiaries, etc.) Within the scope of the requirements and obligations determined with the regulatory and supervisory agencies to ensure the fulfillment of the legal obligations specified in the PDPL as required or required by the legal regulations,
Protection and security of association interests	Conducting necessary audit activities to protect the interests and interests of the association, Ensuring the legal security of people who are in contact with our association, keeping CCTV records to protect the equipment and assets of the Association, taking technical and administrative security measures, carrying out the necessary studies for the development of our activities, implementation and supervision of the workplace rules, planning and execution of social responsibility activities, Protecting 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, to carry out our necessary audits or to fulfill our reporting and other obligations determined by laws and regulations.
Planning and execution of association activities	Determination, planning and implementation of the association's short, medium and long term policies, In line with the purpose of determining and implementing strategies; Conducting communication, market research and social responsibility activities carried out by our association, managing power of attorney and authorization processes

Our Personal Data Processing Purposes	Examples
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.

HOW DO WE USE YOUR PERSONAL DATA FOR MARKETING

Since the marketing activities are not evaluated within the scope of the exceptions regulated in PDPL article 5/2 and article 6/3, As a rule, we always get your consent to process your personal data as part of our marketing activities. Our association can send you communication materials about our activities and campaigns at regular intervals. Such communications can be sent to you through different channels such as email, phone, SMS text messages, mail and third-party social networks.

Sometimes, these communications can be adapted to your preferences to give you the best experience.
(for example, as you tell us about it, based on the results we've drawn from your website visits or based on the links you clicked on our emails).

When required by applicable legislation, we will ask for your permission before starting the above activities. You will also be given the opportunity to revoke (stop) your consent at any time. In particular, you can always stop sending marketing notifications to you by following the unsubscribe instruction included in every email and SMS message.

If you log into a Global Communities account, you may be given the option to change your communication preferences under the relevant section of our website or app. You can always contact us to stop sending you marketing communications (contact details can be found in the section "What are your rights related to your personal data?" Below).

FOR WHAT LEGAL REASONS DO WE PROCESS YOUR PERSONAL DATA?

Law on the Relations of Associations and Foundations with Public Institutions and Organizations, numbered 5072,
Regulation No. 27074 on Blood and Blood Products Blood and Blood Products Law No. 5624, Turkish Code of Obligations No. 6098, Tax Procedure Law No. 213, We operate within the framework of the following legal reasons, which are regulated in article 5 of the PDPL, including electronic commerce legislation:

Legal Reason	Examples
According to PDPL and other legislation in cases where we need to obtain your explicit consent, we process it based on your consent (We would like to remind you that in this case you can withdraw your consent at any time)	We take your consent to carry out our marketing activities.

Legal Reason	Examples
In any case permitted by applicable legislation.	Including the name of the person concerned on the invoice under article 230 of the Tax Procedure Law.
When anyone has an obligation to protect their vital interests.	Giving the health information of the member of the board of directors who has passed out on the board of directors to the doctor.
In cases where we have to contract with you, execute the contract and fulfill our obligations under a contract.	Obtaining the bank account information of the donor within the scope of the donor relationship.
Fulfilling our legal obligations.	Fulfilling our tax obligations, presenting the information requested by the court decision to the court.
If your personal data has been publicized by you	To send us an e-mail to contact you, to write the contact information of the candidate to the website where the job application is collected, the use of personal data that you have publicized through means such as social media channels for the purpose of publication.
Data processing is mandatory for the establishment or protection of a right, using our legal rights and defending against legal claims filed against us	Keeping documents in the nature of proof / evidence and using them when necessary
In cases where our legitimate interests require, provided that it does not harm your fundamental rights and freedoms.	To ensure the security of our association communication networks and information, Conducting our association's activities, determining suspicious transactions and conducting research to comply with our risk rules, To benefit from storage, hosting, maintenance and support services in order to provide IT services in terms of technical and security, Utilize cloud technology to ensure the efficiency of our association's activities and take advantage of technology's possibilities.

Kişisel Verilerinizin açık rıza ile işlendiği hallerde, işbu açık rızanızı geri almanız durumunda söz konusu açık rızaya dayalı işlemenin gerekli olduğu üyelik programından çıkarılacağınızı ve söz konusu işlemeler sayesinde yararlandığınız avantajlardan ilgili tarih itibariyle yararlandırılamayacağınızı önemle belirtmek isteriz.
Where your Personal Data is processed with explicit consent, we would like to emphasize that if you withdraw this explicit consent, you will be removed from the membership program where the explicit consent-based processing is required and that you will not be able to benefit from the benefits provided by these transactions as of the relevant date.

WHEN WE SHARE YOUR PERSONAL DATA?

Transfer of Personal Data in Turkey

Our association is under the responsibility of acting in accordance with the decisions and related regulations envisaged in the PDPL and by the Board regarding the transfer of personal data, especially article 8 of the PDPL. As a rule, personal data and special data of the data owners cannot be transferred to other real persons or legal entities without the express consent of the person concerned.

In addition, transfer is possible without the consent of the person concerned in the situations stipulated in articles 5 and 6 of the PDPL. Our association, in accordance with the conditions stipulated in the PDPL and other relevant legislation and taking the security measures specified in the legislation, (If there is an existing contract signed with the data subject, in the contract in question) Unless otherwise provided by law or other legislation, it may transfer to third parties in Turkey and the economic enterprises of Global Communities.

Transfer of Personal Data Abroad

Our association can transfer personal data to third parties in Turkey, also transfers to abroad by taking the security measures specified in the legislation and in accordance with the conditions stipulated in the Law and other relevant legislation, including the outsourcing, to be processed in Turkey or processed and maintained outside of Turkey. We transfer your personal data abroad by taking necessary technical and administrative measures through cloud computing technology in order to carry out our association activities in the most efficient way and to benefit from the opportunities of technology.

In accordance with PDPL article 9, as a rule, we seek the explicit consent of the data subjects for the transfer of personal data abroad. However, in accordance with PDPL article 9, Provided that one of the conditions regulated in PDPL article 5/2 or article 6/3 exists and the following conditions are met in the foreign country where the personal data will be transferred, It can be transferred abroad without seeking the explicit consent of the owner:

a) Adequate protection is available,
b) In the absence of adequate protection
Data supervisors in Turkey and the relevant foreign country undertake adequate protection in writing and have the Board's permission.

Accordingly, in exceptional cases where explicit consent regarding the transfer of the above-mentioned personal data is not sought, in addition to the non-consensual processing and transfer conditions, it is required to have sufficient protection in the country where the data will be transferred in accordance with PDPL. The Personal Data Protection Board will determine whether adequate protection is provided; if there is not enough protection, Data supervisors in both Turkey and the relevant foreign country must undertake adequate protection in writing and have the permission of the Personal Data Protection Board.

In accordance with this paragraph, please find list for the service providers whose headquarters is abroad and for which we receive support.

- Microsoft
- Watchdog List
- Carbonite
- Kobotoolbox
- Fulcrumpp
- Citrix Podio

- ADP
- SmarterASP.net

Parties Shared in Turkey and Abroad

We do not share your Personal Data except for the special circumstances described here. Access to your Personal Data within Global Communities will be limited only to those who need to know the information for the purposes described in this Policy. To achieve the purposes of collecting your data (for detailed information about these purposes, see "For what purposes do we use your personal data?" Section above), We transfer your Personal Data to the following individuals and institutions:

1. *Service Providers*: While carrying out the activities of our association, it defines the parties to which we have established a business partnership for purposes such as the realization and promotion of the activities of our Association. Like many data supervisors, we provide information and communication technology providers for the most efficient and up-to-date execution of functions and services under some data processing activities, consultancy service providers, SMS and E-mailing service providers, cargo service providers, we can work with trusted third parties such as travel agencies and share data to carry out our activities in this context. This sharing is limited to the purpose of ensuring the establishment and performance of the business partnership is fulfilled. It uses cloud computing technologies to carry out the activities of our association in the most efficient way and to make maximum use of technology. and within this scope, we can process your personal data at home and abroad through companies that offer cloud computing services. The marketing services support company we share can be established abroad and in this context, in accordance with the provisions of PDPL article 8 and article 9, data sharing with abroad is carried out in accordance with the provisions regarding data sharing abroad.

2. *Public institutions and organizations*: We may share your personal data with the relevant official, judicial and administrative authorities, as required by law and legal obligations, or when we need to protect our rights. (e.g. Provincial Health Directorates, Ministry of Health, Ministry of Family and Social Policies, Ministry of Youth and Sports, Disaster and Emergency Management Presidency, Ministry of Interior, Governorate, law enforcement, courts and enforcement offices).

3. *Private Law Persons*: According to the provisions of the relevant legislation, limited personal data sharing can be made for the purpose requested by the private law persons authorized to receive information and documents from our Association (E.g. Occupational Health and Safety Association).

4. Professional consultants and others: Banks, insurance companies, auditors, lawyers, financial advisers and other consultants, With professional consultants, we may share your personal data to the groups of people below.

   • Lawyers
   • Financial Advisors

5. Other parties associated with corporate transactions: In addition, from time to time, executing your Personal Data within the scope of corporate transactions, for example, contracts for the conduct of Association activities, established contractual relations, Firms that we receive services and consultancy in Turkey and abroad in order to ensure the efficiency and security of our association processes, We share with our donors, volunteers, subcontractors, foreign

suppliers, business partners, and other parties associated with corporate transactions such as Global Communities HQ.

HOW LONG DO WE KEEP YOUR PERSONAL DATA?

We retain your personal data only for the time required to fulfill the purpose for which they were collected. We set these times separately for each business process, and if there is no other reason to hide your personal data at the end of the related periods, we destroy your personal data in accordance with PDPL.

When determining the destruction periods of your personal data, we consider the following criteria:

- The time accepted as a general practice in the sector in which the data controller operates, within the scope of the purpose of processing the relevant data category,
- The duration of the legal relationship established with the relevant person, which requires the processing of personal data in the relevant data category,
- The period during which the legitimate interest to be obtained by the data controller will be valid in accordance with the law and the rules of honesty, depending on the purpose of the relevant data category.
- The period during which the risks, costs and responsibilities to be maintained due to the storage of the relevant data category depending on the purpose of the process will continue legally,
- Whether the maximum period to be determined is suitable for keeping the relevant data category accurate and up-to-date, if necessary,
- The period in which the data controller has to store personal data in the relevant data category due to his legal obligation,
- The timeout period set by the data controller to assert a right linked to personal data in the relevant data category.

HOW DO WE ANNIHILATE YOUR PERSONAL DATA?

Although personal data has been processed in accordance with the provisions of the relevant law in accordance with the 138th article of the Turkish Penal Code and the 7th article of the PDPL, in case the reasons requiring processing disappear It is deleted, destroyed or anonymized based on our association's own decision or if the personal data owner has a request in this direction.

In this context, Personal Data Retention and Disposal Policy has been prepared. In accordance with the relevant legislative provisions, our association reserves the right not to fulfill the request of the data subject in cases where it has the right and / or obligation to protect personal data. When personal data is processed in non-automated ways, provided that it is part of any data recording system, the system of physical destruction of the personal data in a way that cannot be used later is applied while the data is deleted / destroyed.

When our association has agreed with a person or organization to process personal data on its behalf, the personal data is securely deleted by that person or organizations, so that it cannot be recovered again. Our association can anonymize personal data when the reasons that require the processing of personal data processed in accordance with the law are eliminated.

DESTRUCTION METHODS OF PERSONAL DATA

Deleting 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 may delete personal data based on its decision or at the request of the personal data subject. 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:

o Identification of personal data that will be the subject of deletion.
o Identification of relevant users for each personal data using the access authorization and control matrix or a similar system.
o Determining the authorities and methods of the related users such as access, retrieval and reuse.
o 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	Description
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 privileges of the users and delete them.
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 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 Found on Paper: Personal data on paper media should be deleted using the blackout method. Dimming process, cutting the personal data on the relevant documents whenever possible, In cases where it is not possible, it is made as invisible to the users by using fixed ink so that it cannot be returned and cannot be read with technological solutions.

Office Files on the Central Server: The file must be deleted with the delete command in the operating system or the relevant user's access rights must 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.

Destruction of Personal Data

Although our association has been processed in accordance with the provisions of the relevant law, In case the reasons requiring 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 Environment	Description
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: Data that is processed in fully or partially automated ways and stored in digital media is deleted / destroyed; The methods for deleting the data from the related software are used in a way that cannot be recovered again.

Secure 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 / destroyed by the person skilled in the art, so that it cannot be recovered again.

Blackout: To make personal data unreadable physically.

Personal Data Destruction Methods

To destroy personal data, It is necessary to identify all the copies containing the data and to destroy them one by one of the following methods depending on the type of systems where the data is available:

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.): Storage media in these 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 disks have ATA (SATA, PATA etc.), SCSI (SCSI Express etc.) interface, using <block erase> command if supported, if it is not supported, it must be destroyed by using the method of disposal proposed by the manufacturer or by using one or more of the appropriate methods specified in (a). iii) Magnetic tape: They are the media that store the data with the help of micro magnet pieces on the flexible band. 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: They 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 cards and fixed memory areas): There are erase commands in the fixed memory areas of portable smartphones, but most do not have an erase 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 destroyed 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: By verifying that all data recording media are removed, it should be destroyed by using one or more of the appropriate methods mentioned in (a). 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 Media: Since the personal data in these environments are permanently and physically written on the medium, the main medium 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 personal data contained in the said systems, it is necessary to encrypt with cryptographic methods and use separate encryption keys where possible for personal data, especially for each cloud solution that is served. 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.

Anonymizing 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 must 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.

In accordance with article 28 of the Personal Data Protection Law; Personal anonymized data can be processed for purposes such as research, planning and statistics. Such transactions are outside the scope of the Personal Data Protection Law and the explicit consent of the personal data owner will not be sought.

<u>Anonymization Methods of Personal Data</u>

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

Anonymize, by removing or altering all direct and / or indirect identifiers in a dataset, preventing the identity of the person concerned from being identified or losing its distinction in a group or crowd in a way 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. Anonymization methods are called

anonymization methods, all of which are carried out with methods such as automatic grouping, masking, derivation, generalization, randomization applied to the records in the data recording system where personal data is kept. 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 of the data in the cluster, instead, changes are made to the entire row or column in the cluster. Thus, while the data changes throughout the data, the values in the fields maintain their original state.

Subtracting 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.

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.

Sectional 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 purchasing wet wipes.

Lower and Upper Limit Coding

The upper and lower nerve coding method is obtained by defining a category for a certain variable by combining the values that fall within 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.

Global Coding

Sampling

In the sampling method, instead of the whole data set, a subset from the set is explained or shared. Thus, the risk of generating accurate predictions about individuals is reduced, 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. 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, only in the relevant dataset are the records of women whose province is Istanbul, and the population registration is removed from the dataset, and anonymization is applied and the data is disclosed or shared, Since the malicious person who has accessed the data cannot predict whether the population record of a woman she knows lives in Istanbul will not be able to make a reliable estimate whether the information she knows is included in the data she has.

Anonymization Methods Providing Irregularity in Value: Unlike the methods mentioned above with methods that provide value irregularity; By changing the existing values, a distortion in the values of the data set is created. 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 Merging

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.

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, to prevent 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.

L-Diversity

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

T-Proximity

Although the L-diversity method provides diversity in personal data, there are cases 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 closeness 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 / processing purpose desired from the data,
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 a data is being anonymized, our association checks whether the data in question re-identifies a person through contracts and risk analyzes by using information known to be within the body of other institutions and organizations to whom it transmits personal data.

Anonymity Assurance

While our association has decided to anonymize a personal data rather than being deleted or destroyed, Anonymity cannot be disrupted by combining an anonymized dataset with a thousand other datasets, not to create a meaningful thousand whole in a way that makes a record singular of a thousand or more than one value, Attention is paid to ensure that the values in the anonymized data set do not merge and produce an assumption or result. 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 eliminating 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 turn back into 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.

HOW DO WE PROTECT YOUR PERSONAL DATA?

In order to protect your personal data and prevent illegal access, the necessary administrative and technical measures are taken by our Association in line with the Personal Data Security Guide published by the Authority for the protection of your personal data, Procedures are organized within the association, lighting and explicit consent texts are prepared and necessary inspections are carried out to ensure the implementation of PDPL provisions in accordance with PDPL article 12/3 or outsourcing. These audit results are evaluated within the scope of the internal functioning of the Association and necessary activities are carried out to improve the measures taken.

Your personal data mentioned above, It can be kept in both digital and physical environment by being transferred to the physical archives and information systems of our association and / or suppliers. The technical and administrative measures taken to ensure the security of personal data are described in detail under two headings below.

Technical Measures

We use generally accepted standard technologies and operational security methods, including standard technology called Secure Socket Layer (SSL), to protect the collected personal information. However, due to the feature of the Internet, information can be accessed by unauthorized people over the networks without the necessary security measures. We take technical and administrative measures to protect your data from risks such as destruction, loss, falsification, unauthorized disclosure or unauthorized access, depending on the current state of technology, the cost of technological implementation and the nature of the data to be protected. In this context, we conclude agreements regarding data security with the service providers we work with. You can reach detailed information by contacting kvkkiletisim@globalcommunities.org.

1) Ensuring Cyber Security: We use cyber security products to ensure personal data security, but the technical measures we receive are not limited to this. With the measures such as firewall and gateway, the first line of defense is created against attacks from environments such as the Internet. However, almost every software and hardware undergoes some setup and configuration processes. Taking into account that

some commonly used software, especially older versions, may have documented vulnerabilities, unused software and services are removed from the devices. For this reason, it is primarily preferred to delete unused software and services instead of keeping them up-to-date, because of their ease. With patch management and software updates, it is ensured that the software and hardware are working properly and that the security measures taken for the systems are checked regularly.

2) Access Limitations: Access powers to systems containing personal data are limited and regularly reviewed. In this context, employees are given access authorization to the extent necessary for their work and duties, as well as their authority and responsibilities, and access to relevant systems is provided by using a user name and password. When creating these passwords and passwords, combinations consisting of uppercase letters, numbers and symbols are preferred instead of numbers or letter sequences related to personal information that can be easily guessed.
Accordingly, an access authorization and control matrix is created.

3) Encryption: In addition to the use of strong passwords and passwords, limiting the number of password entry attempts to protect against common attacks such as brute force algorithm (BFA) usage, ensuring that passwords and passwords are changed at regular intervals, Access is limited to methods such as opening the manager account and admin authority only when needed, and for employees who are dismissed from the data officer, such as deleting the account or closing entries without losing time.

4) Anti-Virus Software: In addition, products such as antivirus, anti-spam, which regularly scan the information system network and detect hazards are used to protect against malware. In addition, these are kept up to date and the required files are regularly scanned. If personal data is to be provided from different websites and / or mobile application channels, connections are provided via SSL or a more secure way.

5) Tracking of Personal Data Security: Checking which software and services are working in IT networks, Determining whether there is an infiltration or not movement in the information networks, Recording all transaction transactions of all users regularly (such as log records), Reporting security problems as quickly as possible, The above transactions are done. Again, an official reporting procedure is created for employees to report security weaknesses in systems and services or threats that use them. Evidence is collected and securely stored in undesirable events such as computer system crash, malicious software, denial of service attack, missing or incorrect data entry, violations of privacy and integrity, and misuse of the information system.

6) Ensuring the Security of Media Containing Personal Data: If personal data is stored on devices or on paper in the premises of the data responsible, Physical security measures are taken against threats such as theft or loss of these devices and papers. Physical environments in which personal data are contained are protected against external risks (fire, flood etc.) with appropriate methods and the entry / exit to these environments are taken under control.

If the personal data are in electronic form, To prevent personal data security breaches, access between network components can be limited or components separated. For example, if personal data is processed in this area by limiting it to a particular part of the network in use reserved only for this purpose, available resources can be reserved for the security of this limited space, not just for the entire network.

Precautions at the same level are also taken for paper media, electronic media and devices located outside the Association campus that contain personal data belonging to the Association. As a matter of fact, although personal data security violations often occur due to theft and loss of devices (laptop, mobile phone, flash disk, etc.) containing personal data, personal data to be transmitted by e-mail or mail is sent carefully and with sufficient precautions. In case employees have access to the information system network with their personal electronic devices, adequate security measures are taken for them.

The method of using access control authorization and / or encryption methods is applied in case of loss or theft of devices containing personal data. In this context, the encryption key is stored in an environment accessible only to authorized persons and unauthorized access is prevented.

Documents in the paper medium containing personal data are also kept locked up and in an environment accessible only to authorized persons, unauthorized access to such documents is prevented.

In accordance with PDPL article 12, our association notifies this situation to the Personal Data Protection Board and data owners as soon as possible if the personal data is obtained by others in illegal ways. The Personal Data Protection Board may announce this situation on the website or by any other method, if it deems necessary.

7) Storing Personal Data in the Cloud: If the personal data are stored in the cloud, the Association should evaluate whether the security measures taken by the cloud storage service provider are sufficient and appropriate. In this context, two-step authentication control is applied for knowing what the personal data stored in the cloud is in detail, backing up, ensuring synchronization and remote access if this personal data is required.

During the storage and use of personal data contained in these systems, encryption is encrypted with cryptographic methods, encrypted and discarded to cloud environments, wherever possible for personal data, encryption keys are used separately for each cloud solution where services are provided. When the cloud computing service relationship ends all copies of encryption keys that can make personal data available are destroyed. Access to data storage areas with personal data is logged and improper accesses or access attempts are instantly communicated to those concerned.

8) Information Technology Systems Procurement, Development and Maintenance: The security requirements are taken into consideration when determining the needs related to the supply, development or improvement of existing systems by the association.

9) Backing Up of Personal Data: In cases such as personal data being damaged, destroyed, stolen or lost due to any reason, the Association ensures that it becomes operational as soon as possible using the backed up data. The backed up personal data can only be accessed by the system administrator, and data set backups are kept out of the network.

Administrative Measures

- All the activities carried out by our association were analyzed in detail in all business units and as a result of this analysis, a process-based personal data processing inventory was prepared. Risky areas in this inventory are determined and necessary legal and technical measures are taken continuously. (Example; Documents to be prepared within the scope of PDPL were prepared considering the risks in this inventory)

- Personal data processing activities carried out by our association are audited by information security systems, technical systems and legal methods. Policies and procedures regarding personal data security are determined and regular controls are carried out within this scope.

- Our association may receive services from external service providers from time to time to meet the information technology needs. In this case, the transaction is carried out by making sure that the external data processing providers provide at least the security measures provided by our Association. In this

case, this contract, signed by signing a written contract with Data Processor, includes at least the following issues:

- The Data Processor acting only in accordance with the data processing purpose and scope specified in the contract and in accordance with the PDPL and other legislation, in accordance with the instructions of the Data Controller,

- Act in accordance with Personal Data Retention and Destruction Policy,

- Subject to the obligation to keep an indefinite secret of the personal data processed by the Data Processor,

- In the event of any data breach, the Data Processor is obliged to report this to the Data Supervisor immediately,

- Our Association will make or have the necessary inspections on the Data Processing's systems containing personal data, examine the reports resulting from the inspection and the service provider company on site,

- It will take the necessary technical and administrative measures for the security of personal data; and

- In addition, as the quality of the relationship between Data Processor and us allows, the categories and types of personal data transferred to the Data Processor are also specified in a separate article.

- As emphasized by the institution's guides and publications, personal data are reduced as much as possible within the framework of the data minimization principle and personal data that are not necessary, outdated and do not serve a purpose are not collected and if it was collected in the period before PDPL, it is destroyed in accordance with the Personal Data Retention and Destruction Policy.
- Specialist personnel are employed for technical issues.
- Our Association has determined provisions regarding confidentiality and data security in the Labor Contracts to be signed during the recruitment processes of its employees and asks employees to comply with these provisions.
- Employees are regularly informed and trained on the protection of personal data and taking necessary measures in accordance with this law. The roles and responsibilities of the employees were revised in this context and job descriptions were revised.
- Technical measures are taken in accordance with technological developments, the measures taken are periodically checked, updated and renewed.
- Access authorizations are limited and the authorities are regularly reviewed.
- The technical measures taken are regularly reported to their officials, and the risk issues are reviewed and efforts are made to produce the necessary technological solutions.
- Software and hardware including virus protection systems and firewalls are being installed.
- Backup programs are used to ensure that personal data is stored securely.
- Security systems for hiding areas are used, technical measures are periodically reported to the relevant person, as required by internal controls, and necessary technological solutions are produced by reassessing the risk poses. The files / outputs stored in the physical environment are stored through the supplier companies studied and subsequently destroyed in accordance with the established procedures.
- The subject of Protection of Personal Data is also owned by the senior management, a special Committee has been formed in this regard (Personal Data Protection Committee) and it has started to work. A management policy that regulates the working rules of the Association Personal Data

Protection Committee was put into effect within the Association and the duties of the Personal Data Protection Committee were explained in detail.

HOW DO WE PROTECT YOUR PRIVATE QUALIFIED PERSONAL DATA ?

A separate policy regarding the processing and protection of special quality personal data has been prepared and put into effect.

PDPL article 6 has been organized as personal data of special quality and subject the processing of these data to more sensitive protection When the data on foundation or union membership race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, disguise and dress, association, health, sexual life, criminal conviction and security measures and biometric and genetic data are processed illegally Since they have the risk of causing victimization or discrimination of individuals.

Our association, in accordance with the 10th article of PDPL, It illuminates the Relevant Persons during the acquisition of special quality personal data. Special quality personal data are processed by taking appropriate measures for PDPL and by performing / having the necessary inspections. As a rule, another requirement of processing of personal data of special quality is the express consent of the data subject. Our association offers the opportunity for the data owners to express their open consent on a specific subject, based on information and with free will.

Our association, as a rule, takes the express consent of the Relevant Persons in writing to process special personal data. However, in accordance with PDPL article 6/3, In case of any of the conditions specified in PDPL article 5/2, the explicit consent of the Relevant Persons is not sought. Besides PDPL article 6/3, protection of public health of personal data related to health and sexual life, Persons under obligation to keep secrets for the purpose of carrying out preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing or authorized institutions and organizations can be processed without the explicit consent of the person concerned.

Regardless of the reason, general data processing principles are always taken into consideration and complied with.

Our association takes special precautions to ensure the security of special quality personal data. Due to the principle of data minimization, special personal data are not collected unless necessary for the relevant business process and processed only when necessary. In case of processing of special data, special technical and administrative measures are taken to comply with the legal obligations and to comply with the measures determined by the Personal Data Protection Board.

WHAT ARE YOUR RIGHTS ABOUT YOUR PERSONAL DATA?

As data owners under PDPL article 11, you have the following rights regarding your personal data:

- To find out whether your personal data is processed by our Association,
- Requesting information if your personal data has been processed,
- To learn the purpose of processing your personal data and whether they are used in accordance with their purpose,
- To know the third parties to whom your personal data are transferred domestically or abroad,
- In case your personal data are incomplete or incorrectly processed, request that they be corrected and request the notification of the transaction made within this scope to third parties to whom your personal data is transferred,

- Although processed in accordance with PDPL and other relevant legal provisions, requesting the erasure or destruction of your personal data in case the reasons requiring its processing disappear, and requesting the process performed within this scope to be notified to third parties to whom your personal data is transferred,
- To object to the emergence of a result against you by analyzing the processed data exclusively through automated systems,
- Requesting the elimination of the loss if you suffer damage due to illegal processing of your personal data.

You can send these requests to our Association free of charge in accordance with the Application Communiqué, as follows:

1) After filling the form which is taken from https://globalcommunities.org.tr/ and signing it as wet signed. Transmission to address 15 Temmuz mah. 148031 nolu sok. No:3 A ve B blok, Şehitkamil/Gaziantep/Turkey personally (We would like to remind you that your identity will need to be presented).
2) After filling the form which is taken from https://globalcommunities.org.tr/ signing it as wet signed. Sending to the address Global Communities Inc. Turkey representative office 15 Temmuz mah. 148031 nolu sok. No:3 A ve B blok, Şehitkamil/Gaziantep/Turkey through a notary.
3) After filling in the application form which is taken from https://globalcommunities.org.tr/ and signing it with your "secure electronic signature" under the Electronic Signature Law No. 5070 sending the secure electronic signed form to **chfinternational@hs02.kep.tr** by registered e-mail.
4) To send to our Association in writing by using your e-mail address which was previously notified and registered in the system of our Association.

In the application;

Name, surname and signature if the application is in writing, TR Identity Number for Turkish Republic citizens, nationality, passport number or identification number, if any, the place of residence or business address subject to notification, e-mail address based on notification, if any, phone and fax number, subject of demand, must be found. Information and documents related to the subject are also added to the application.

It is not possible to request third parties on behalf of personal data owners. In order for a person other than the personal data owner to make a request, a private signed and notarized copy of the private power of attorney issued by the personal data owner on behalf of the person to apply must be found. In the application that contains your explanations about the right that you have as a personal data owner and that you have made and requested to use your rights mentioned above; the matter you request is clear and understandable, If the subject you are requesting is related to your person or you are acting on behalf of someone else, you should be specially authorized and document your authority, the application must include identification and address information and documents that prove your identity must be attached to the application.

Applications within this scope will be concluded within the shortest possible time frame and within 30 days. These applications are free. However, in case the transaction also requires a cost, the fee in the tariff determined by the Personal Data Protection Board may be charged.

If the personal data owner transmits his request to our Association in accordance with the prescribed procedure, our Association will conclude the request free of charge as soon as possible and within thirty days at the latest, depending on the nature of the request. However, in the event that the transaction requires a separate cost, the fee determined by the Personal Data Protection Board of the applicant will be charged by our Association. Our association may request information from the person concerned to determine

whether the applicant has personal data. Our association may ask questions regarding the application to the personal data owner in order to clarify the issues in the application of the personal data owner.

According to PDPL article 14 In case your application is rejected by our association, if you find our answer insufficient or if we do not respond to the application in due time; You can complain to the Personal Data Protection Board within thirty days, and in any case sixty days from the date of application of our association.

WHAT ARE THE CONDITIONS WHICH DATA OWNERS MAY NOT CLAIM THE RIGHTS?

Personal data owners, pursuant to Article 28 of the PDPL Since the following cases are excluded from the scope of PDPL, they cannot claim the above-mentioned rights of personal data subjects on these issues:

- Processing of personal data for purposes such as research, planning and statistics by making it anonymous with official statistics.
- Processing of personal data for art, history, literature or scientific purposes or within the scope of freedom of expression, provided that it does not violate national defense, national security, public security, public order, economic security, privacy or personal rights, or constitute a crime.
- Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to provide national defense, national security, public security, public order or economic security.
- Processing of personal data by judicial authorities or enforcement authorities regarding investigations, prosecutions, trials or execution proceedings.

As per article 28/2 of PDPL; Personal data holders cannot claim their other rights, except for the right to demand compensation for damage, in the following cases:

- Personal data processing is necessary for the prevention of crime or criminal investigation
- Processing of personal data personalized by the personal data owner.
- The fact that personal data processing is necessary for the disciplinary investigation or prosecution by the authorized and authorized public institutions and organizations and the professional institutions that are public institutions based on the authority given by the law.
- Personal data processing is necessary for the protection of the State's economic and financial interests in relation to budget, tax and financial matters.

OTHER ISSUES

As described in detail above, your personal data can be stored and stored, classified as required by market research, operational processes and marketing activities, can be updated in different periods and transferred to third parties and / or suppliers and / or service providers required by the service within the framework of laws and confidentiality principles, as permitted by the legislation, In accordance with the policies we are affiliated with and for reasons envisaged by other authorities, records and documents may be arranged to be based on the transaction in electronic or paper environment that can be transferred, stored, processed by reporting.

If there is a discrepancy between the PDPL and other relevant legislative provisions and this Policy, the PDPL and other relevant legislative provisions will be applied first.

This Policy prepared by our Association has entered into force in accordance with the decision taken by the Board of Directors of Global Communities.

We would like to remind you that we can make updates to this Policy due to legislative provisions that may change over time and changes that may occur in our Association policies. We will post the most current version of the Policy on our website.

The User / Users have accepted, declared and undertaken that the following issues will be deemed irrevocable, pursuant to Article 193 of the Civil Procedure Law: read this Personal Data Protection Policy before entering the website, they will comply with all the issues mentioned here, all electronic media and computer records of the content on the website and our Association

Effective date: 23.03.2021

Version: 0

ANNEX – ABBREVIATIONS

ABBREVIATIONS	
Law No. 5651	**Editing of the Broadcasts on the Internet, which came into force after being published in the Official Gazette No. 26530 dated 23 May 2007. Law on Combating Crimes Committed through These Publications**
Constitution	**The Constitution of the Republic of Turkey, published in the Official Gazette No. 17863 dated 9 November 1982 Constitution of the Republic of Turkey dated November 7, 1982 numbered 2709**
Application Notification	**Communiqué on the Procedures and Principles of Application to the Data Supervisor, published in the Official Gazette No. 30356 dated March 10, 2018**
Contact / Relevant Persons or Data Owner	**Customers of donors, volunteers, beneficiaries and / or economic enterprises that Global Communities are related to, its corporate customers, business partners, shareholders, officials, candidate employees, trainees, visitors, suppliers, the employees of the institutions that they work in cooperation, It refers to the real person whose personal data is processed, such as third parties and others, but not limited to those listed here.**
Regulation on the deletion, destruction or anonymization of Personal Data	**Regulation on the Deletion, Destruction, or Anonymization of Personal Data published in the Official Gazette No. 30224 dated October 28, 2017 and entered into force on January 1, 2018.**
PDPL	**Law on the Protection of Personal Data, which came into force after being published in the Official Gazette dated 7 April 2016 and numbered 29677.**
Personal Data Protection Board	**Personal Data Protection Board**
Personal Data Protection Authority	**Personal Data Protection Authority**
article	**Article**
Example	**Sample**
Policy	**These Global Communities Personal Data Protection and Privacy Policy**
Associations / Organizations	**Global Communities Inc. Turkey Representative Office**
Turkish Criminal Code	**Turkish Penal Code, published in the Official Gazette No. 25611 dated 12 October 2004; Turkish Penal Code No. 5237 of 26 September 2004**