THE POLICY OF PROTECTION AND PROCESSING OF PERSONAL DATA OF GLOBAL COMMUNITIES INC. TURKEY REPRESENTATIVES OFFICE EMPLOYEES

VERSION

Version No	Version Date	Change Description
V-1	November 2020	

CONTENT

1. PURPOSE AND SCOPE

The Global Communities Inc. Turkey Representative Office ("Global Communities" or "Association") makes every effort to comply with all applicable legislation regarding the processing and protection of personal data.

Global Communities Employee Personal Data Protection and Processing Policy ("Employee PDP Policy") and the procedures and principles in force regarding the protection and processing of personal data are determined. This Policy is part of the Employee Disclosure Text and Employee Explicit Consent Text documents that are presented to employees at the time of recruitment and should be considered together with these two documents regarding the processing of personal data of employees.

In line with the importance given by Global Communities to the protection of personal data, the Employee PDP Policy sets out the principles regarding the compliance of activities related to the processing of personal data of Global Communities employees with the Law No. 6698 on Protection of Personal Data ("PDPL").

Employee PDP Policy is for employees whose personal data are processed by Global Communities, and issues related to Global Communities visitors, former employees, employee candidates, customers, business partners, suppliers and employees and other third parties are also covered in the Global Communities Personal Data Protection Policy ("**Global Communities PDP Policy**") published in https://globalcommunities.org.tr/politikalar/.

2. PRINCIPLES OF EMPLOYEE PDP POLICY

2.1. GENERAL PRINCIPLES

The Employee PDP Policy is included in https://globalcommunities.org.tr/politikalar/ and is accessible to Employees. In line with the changes and innovations to be made in the relevant legislation, the changes to be made in the Employee PDP Policy will be accessible to the data owners so that the Employee data owners can easily access them.

Global Communities acknowledge that the applicable legislation will find application if there is a conflict between the legislation in force regarding the protection and processing of personal data and this Employee PDP Policy.

2.2. PEOPLE MANAGED BY EMPLOYEE PDP POLICY

The term Employee in this Policy refers to all employees on the Global Communities payroll. Employees are subject to the principles regulated by the Employee PDP Policy until their business relationship with Global Communities ends.

3. PRINCIPLES ADOPTED BY GLOBAL COMMUNITIES

Global Communities comply with (i) basic principles, (ii) personal data processing conditions and (iii) special quality personal data processing conditions while conducting the activities of processing personal data of Employees.

3.1. COMPLIANCE WITH BASIC PRINCIPLES

Global Communities adopt the following basic principles in order to ensure compliance and maintain compliance with the protection of Employees' personal data:

(1) Processing personal data in accordance with law and integrity rules

In accordance with the legislation on protection of personal data, Global Communities conduct their personal data processing activities in accordance with the law and the integrity rule especially the Constitution of the Republic of Turkey.

(2) Ensuring the accuracy and up-to-datedness of the processed personal data

All necessary administrative and technical measures are taken by the Global Communities to ensure the accuracy and up-to-datedness of personal data within the technical possibilities while processing the personal data of the Employees. In this context, Global Communities has established mechanisms to correct and verify accuracy of employee personal data owners if their personal data are incorrect.

(3) Processing personal data in a connected, limited and measured manner

The personal data of the Employees are processed by the Global Communities in connection with the data processing conditions and to the extent necessary for the realization of the data processing purposes. In this context, the purpose of personal data processing is determined before the personal data processing activity is started and data processing activity is not carried out with the assumption that it can be used in the future.

(4) Maintaining personal data for the period required by the relevant legislation or for the purpose for which they are processed

Global Communities retains the personal data of the employees limited to the time stipulated in the relevant legislation or required by the purpose of data processing. Accordingly, personal data is deleted, destructed or anonymized by Global Communities if the period stipulated in the legislation expires or the reasons requiring the processing of personal data disappear. Personal data are not retained by Global Communities, based on the possibility of future use.

3.2. COMPLIANCE WITH PERSONAL DATA PROCESSING TERMS

Global Communities execute the personal data of the Employees in accordance with the data processing conditions set out in the 5th article of the PDPL. In this context, the personal data processing activities carried out are carried out in the presence of the personal data processing conditions listed below:

(1) Presence of Explicit Consent of Personal Data Owner

Personal data processing is carried out by Global Communities, if the employees approve the processing of data about themselves freely, with sufficient knowledge on the subject, without any hesitation and only limited to that process.

(2) The Personal Data Processing Activity Is Clearly Foreseen In The Laws

In the event of a clear regulation of laws relating to personal data processing activities, Personal Data processing activities of the Employees may be carried out by Global Communities without consent, limited to the relevant legal regulation.

(3) Failure to Obtain Explicit Consent of the Data Owner Working Due to Actual Impossibility and Obligatory Personal Data Processing

In cases where the employee cannot explain his consent or his consent is not valid, if processing personal data is mandatory to protect individuals' life or body integrity, data processing is carried out by Global Communities in this context.

(4) The Personal Data Processing Activity Is Directly Related To The Establishment Or Execution Of A Contract

In cases where it is directly related to the establishment or performance of a contract between the employees and the Global Communities, if it is necessary to process the personal data of the parties to the contract, the data processing activity is carried out by the Global Communities.

(5) Personal Data Processing Activity Must be Required for Global Communities to Fulfill their Legal Obligations

In case of the legal obligation of Global Communities, which has adopted the necessary sensitivity to comply with the law as an Association policy, the fulfillment of the legal obligation is carried out personal data processing.

(6) Data Owner Making His/her Personal Data Public

The personal data (publicly disclosed in any way) of the Employees themselves are processed by Global Communities for the purpose of being publicized.

(7) Necessity of Data Processing For the Establishment, Use or Protection of a Right

In the event that the processing of personal data is mandatory for the establishment, use or protection of a right, the Personal Data of the Employees are processed by the Global Communities in parallel with this obligation.

(8) Necessity of Execution of Personal Data Processing for the Legitimate Interests of Global Communities Provided Not to Damage the Fundamental Rights and Freedoms of the Data Owner

For the legitimate interests of Global Communities, if personal data processing is mandatory, data processing can be carried out if the fundamental rights and freedoms of the employee data owner are not harmed. In this context, in order to determine the existence of the condition in question, the "balance test" application, which is accepted by Global Communities in the regulation, is carried out.

3.3. COMPLIANCE WITH SPECIAL QUALITY PERSONAL DATA PROCESSING CONDITIONS

The Global Communities also place special emphasis on the processing of special personal data that are at risk of discrimination when processed illegally. In this context, firstly, it is determined whether there are any data processing conditions in the processing of special personal data of the Employees, and after ensuring the existence of the lawfulness requirement, data processing activity is carried out.

Special quality personal data can be processed by Global Communities, in exceptional cases stated in article 5/2 of PDPL, without seeking explicit consent, provided that adequate measures are determined by the PDP Board.

However, when processing personal data about the health and sexual life of the Employees, explicit consent is absolutely obtained.

3.4. COMPLIANCE WITH PERSONAL DATA TRANSFER CONDITIONS

Global Communities act in accordance with the personal data transfer conditions set out in the PDPL Articles 8 and 9 in the transfer of personal data of the Employees.

(1) Transfer of Employees' Personal Data in Turkey

In accordance with the 8th article of PDPL, the Global Communities act in accordance with the data processing conditions in the data transfer activities to be carried out domestically.

(2) Transfer of Employees' Personal Data Abroad

As per article 9 of PDPL, personal data can be exported abroad by Global Communities (i) in accordance with personal data processing requirements and (ii) with data officers undertaking adequate protection in writing and having the permission of the PDP Board in Turkey and in the foreign country concerned if the country to be transferred is from countries with sufficient protection declared by the PDP Board or if there is not enough

protection in the relevant foreign country. In this context, detailed information is included in the text of Employee Clarification.

4. LIGHTING OF PERSONAL DATA OWNERS

Global Communities carry out the necessary processes to ensure that the Employees are informed during the acquisition of their personal data, in accordance with Article 10 of the PDPL. In this context, the following information is included in the clarification texts presented to the Employees by Global Communities:

(1) Association title,
(2) For what purpose the Personal Data of the Employees will be processed by the Global Communities,
(3) To whom and for what purpose the processed personal data can be transferred,
(4) The method and legal reason of collecting personal data,
(5) The rights that Employees have due to being data owner;
- To find out whether personal data is processed,
- If personal data is processed, requesting information about it,
- Learning the purpose of processing personal data and whether they are used in accordance with its purpose,
- To know the third parties to whom personal data are transferred domestically or abroad,
- In the event that personal data are incomplete or incorrectly processed, to request their correction and to notify the third parties to whom the transaction has been transferred,
- Requesting the deletion or destruction of personal data within the framework of the foreseen conditions and requesting the transaction to be notified to the third parties to whom the personal data has been transferred,
- To object to the emergence of a result against the person by analyzing the processed data exclusively through automated systems,
- Requesting the elimination of the loss in the event that personal data is damaged due to illegal processing.

5. OUR POLICY ON COOKIES

For more information about how we use cookies and other tracking technologies, please read our cookie policy. Generally, “cookie” is the name given to information stored on the user's computer by an Internet service provider. The information contained in the cookies can be used when the user returns to the website in question. Cookies can contain a variety of information, including how many times the user has entered the site in question. Using individual session cookies for each user, we can monitor how you use the site during a single session. Thanks to cookies, we can determine which browser you use and offer you some special services.

Information stored in cookies may include the date of visit, the time of visit, the pages watched, the time spent in the Online transactions Center, and the sites visited the Online Operations Center just before or after the visit. The data collected through these cookies used during the visit to the Online Transactions Center can be evaluated, and then advertisements for products that you may potentially be interested in during your visit to other websites can be shown. It is possible to block cookies via your internet browser.

You can learn how to prevent your computer from receiving cookies using the “help” function found in most browsers, you can understand whether the cookie is sent or not and disable them completely. However, we would like to remind you that if you disable cookies, you will not be able to use this site fully.

This site uses cookies for a variety of purposes, including:

- Accessing certain information to provide you with personalized content upon entering the site;
- Tracking your preferences you specify while using this site, such as your preferred date and number formats. We value the privacy of your information. In order to protect the privacy and security of your confidential information at the highest possible level, we apply the following rules:
- This site does not always have 'cookies' on your disk drive. Cookies are removed when you close your browser or leave the site.
- The information in all cookies sent from this site to your computer is sent encrypted.

6. PROCESSING PERSONAL DATA THROUGH CLOSED CIRCUIT CAMERA RECORDING

Security cameras are used to ensure the safety of our association and facilities and personal data is processed in this way. Our association has purposes to increase the quality of the service provided within the scope of the monitoring activity with the security camera, to ensure the security of life and property of the physical locations of the Association and the persons in the Association, to prevent abuse, and to protect the legitimate interests of the data owners.

Personal data processing activities conducted by our association with security cameras are carried out in accordance with the Constitution, PDPL, Law No. 5188 on Private Security Services and related 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. Only a certain number of Association personnel access CCTV camera images, and these authorizations are regularly reviewed. Staff who have access to these records sign a commitment to protect personal data in a lawful manner.

7. HOW WE DESTROY YOUR PERSONAL DATA?

In line with the 138th article of the Turkish Penal Code and the 7th article of the PDPL, although personal data has been processed in accordance with the relevant legal provisions, 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. 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 in accordance with the relevant legislation provisions. 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, which cannot be used later, is applied while deleting / destroying the data. 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.

You can access all the details regarding the destruction of your personal data by examining the Global Communities Personal Data Retention and Destruction Policy at https://globalcommunities.org.tr/politikalar/.

8. HOW DO WE PROTECT YOUR PERSONAL DATA?

In order to protect your personal data and prevent illegal access, in line with the Personal Data Security Guide published by the PDP Authority, the necessary administrative and technical measures are taken by our Association, procedures are organized within the Association, clarification and explicit consent texts are prepared, and necessary inspections are carried out in order to ensure the implementation of the PDPL provisions in accordance with PDPL Article 12/3, or they are made through outsourcing services. 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. In order to prevent personal data from being disclosed, accessed, transmitted or other security deficiencies that may occur in other ways, we attach special importance to taking necessary measures according to the nature of the data to be protected within the possibilities.

Your personal data mentioned above can be transferred to the physical archives and information systems of our Association and / or our suppliers, and can be kept under both digital and physical environment. 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 find detailed information about these service providers on https://globalcommunities.org.tr/.

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 using a username and password. While these passwords are being created, it is provided to choose combinations consisting of uppercase letters, numbers and symbols rather than numbers or letter sequences related to personal information and which can be easily guessed. Accordingly, an access authorization and control matrix is created.

3) Encryption: In addition to the use of strong passwords, it is time to limit the number of password entry attempts to protect against common attacks such as the use of brute force algorithm (BFA), to ensure that passwords are changed at regular intervals, to open the administrator account and admin authority only when needed, and for employees who are dismissed from the data controller. Access is limited by methods such as deletion of the account or closing entries without losing.

4) Antivirus Software: In addition, products such as antivirus, antispam, which regularly scan the information system network and detect hazards are used to protect against malware, and these are kept up-to-date and the required files are scanned regularly. If personal data is to be obtained 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 information networks, determining whether there is a leak in or should not occur in information networks, Recording all transaction records of all users regularly (such as log records), Reporting security problems as quickly as possible. 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) Securing Media Containing Personal Data: If personal data is stored on devices located on the premises of data officers or on the media, 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 is in electronic environment, access can be limited between the network components or separation of the components to prevent the violation of personal data security. For example, if personal data is processed in this area by restricting only a certain part of the network in use for this purpose, the available resources may be reserved for the security of this limited area, not just for the entire network.

   Measures 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 transferred 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 use 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 and in an environment accessible only to authorized persons, unauthorized access to these documents is prevented.

Our association notifies PDP Board and data owners as soon as possible if personal data are obtained by others illegally in accordance with article 12 of PDPL. PDP Board may announce this situation on its 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 inappropriate 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) Backup 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. (For example, documents that should 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 the Data Processor, includes at least the following issues:
    - Data Processor acting in accordance with the data processing purpose and scope specified in the contract and in accordance with PDPL and other legislation only in accordance with the instructions of the Data Controller,
    - Act in accordance with the Personal Data Retention and Destruction Policy,

  - Data processor's obligation to keep an indefinite secret of the personal data it processes,
  - 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 systems of Data Processor containing personal data, examine the reports resulting from the inspection and the service provider company on site,
  - Taking necessary technical and administrative measures for the security of personal data; and
  - In addition, as the nature of the relationship between Data Processor and our relationship allows, the categories and types of personal data transferred to the Data Processor are also specified in a separate article.

- As emphasized in the guides and publications of the Institution, within the framework of data minimization principle, personal data is reduced as much as possible, personal data that is not necessary, outdated and does not serve a purpose are 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 in technical matters.
- Our Association has determined provisions regarding the confidentiality and data security in the Labor Contracts to be signed during the recruitment processes of its employees and requests the employees to comply with these provisions. Employees are regularly informed and trained on the protection of personal data law 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 privileges are restricted and they 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 in accordance with the internal controls, and the 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 (PDP Committee) and has started to work. A management policy that regulates the working rules of the Association PDP Committee was put into force within the Association and the duties of the PDP Committee were explained in detail.
- The operation of the technical and administrative measures taken within the scope of protection and security of personal data by the Global Communities is supervised and practices that will ensure the continuity of the operation are carried out. The results of the audit activities carried out in this context are reported to the relevant department within the Global Communities. In line with the audit results, activities to ensure the development and improvement of the measures taken for data protection are carried out.
- As part of the personal data processing activity carried out by the Global Communities, if the personal data is unlawfully obtained by unauthorized persons, the situation will be reported to the PDP Board and the relevant data owners without delay.

9. 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.

When processed unlawfully data on race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, disguise and dress, association, foundation or union membership, health, sex life, criminal conviction and security measures, and biometric and genetic data, PDPL article 6 has organized it as a personal data with special quality as it carries the risk of causing victimization or discrimination of individuals and subjected the processing of this data to more sensitive protection.

In accordance with the 10th article of PDPL, our association enlightens the concerned 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 data owners the opportunity to express their explicit 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, pursuant to PDPL article 6/3, the explicit consent of the Relevant Persons is not sought in the presence of any of the conditions specified in PDPL article 5/2. In addition, PDPL article 6/3 means individuals or authorized institutions who are under obligation to keep secrets for the purpose of protecting the public health of health and sexual life, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing. It regulates that it can be processed by organizations without explicit consent of the 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. In accordance with the data minimization principle, special personal data are not collected unless necessary for the relevant association's activity process and are 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 PDP Board.

10. FINALIZATION OF EMPLOYEES DEMANDS FOR PERSONAL DATA

In the case of PDPL, as the Global Communities data supervisor, if the Employees submit their requests regarding their personal data arising from their data ownership to the Association through the **Global Communities Data Owner Application Form** located at https://globalcommunities.org.tr/politikalar/. In accordance with Article 13, it carries out the necessary processes to ensure that the request is finalized as soon as possible and within thirty (30) days at the latest.

Global Communities may request information to determine whether the applicant is the owner of the personal data subject to the application, within the scope of ensuring data security. Our association may also ask questions regarding the application of the personal data owner to ensure that the application of the personal data owner is concluded in accordance with the request.

In cases such as the application of the data subject made by the employee, the possibility of blocking the rights and freedoms of other people, requiring disproportionate effort, and information being public information, the request may be rejected by the Global Communities by explaining its justification.

11. RIGHTS OF EMPLOYEES FOR PERSONAL DATA

Pursuant to Article 11 of the PDPL, Employees can apply to our Association with **the Global Communities Data Owner Application Form** and request the following issues:

(1) Learning whether personal data is processed or not,

(2) If the personal data is processed, requesting information about it,
(3) Learning the purpose of processing personal data and whether it is used in accordance with its purpose,
(4) Learning the third parties whose personal data are transferred domestically or abroad,
(5) In the event that personal data are incomplete or incorrectly processed, requesting their correction and to request notification of the transaction performed within this scope to third parties to whom personal data is transferred,
(6) Requesting that the personal data be deleted, destroyed or anonymized and the notification made in this context is notified to the third parties to whom personal data is transferred, even if the reasons requiring its processing disappear, although it has been processed in accordance with the provisions of PDPL and other relevant laws,
(7) Objecting to the emergence of a result against you by analyzing the processed data exclusively through automated systems,
(8) Requesting the removal of the damage in case the personal data is damaged due to the illegal processing of the data.

Legislation Requirements except the Rights of Personal Data Owners

Pursuant to Article 28 of PDPL, since the following situations are not covered by PDPL, personal data owners will not be able to claim their rights in the following subjects:

(1) 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.
(2) Processing personal data for purposes such as research, planning and statistics by making it anonymous with official statistics.
(3) 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.
(4) Processing of personal data by judicial authorities or enforcement authorities regarding investigations, prosecutions, trials or execution proceedings.

Pursuant to Article 28/2 of the PDPL, it will not be possible for the personal data owners to claim their rights, except for requesting the removal of the damage in the following cases:

(1) Necessity of personal data processing for the prevention of crime or for criminal investigation.
(2) Processing of personal data publicized by the personal data owner himself.
(3) The fact that personal data processing is required by the authorized and authorized public institutions and organizations and professional institutions that are public institutions on the basis of the authority given by the law, is required for the execution of auditing or regulation duties and for disciplinary investigation or prosecution.
(4) Necessity of personal data processing for the protection of the State's economic and financial interests in relation to budget, tax and financial matters.

12. UNIT RESPONSIBLE FOR THE PROTECTION AND PROCESSING OF PERSONAL DATA

Within the scope of ensuring, retaining and maintaining compliance with the legislation on protection of personal data by Global Communities, the “Personal Data Protection Committee”, which will

provide the necessary coordination within the association, has been established. The Personal Data Protection Committee is responsible for the establishment and improvement of systems established to ensure unity between Global Communities units and departments, and to ensure compliance of the activities carried out with the legislation of personal data protection. In this context, you should immediately forward requests to obtain information about the protection of personal data transmitted or directed to you.

13. DEFINITIONS

Definitions of terms used in Employee PDP Policy are given below:

Explicit Consent	**:**	Consent to a specific subject, based on information and explained with free will.
Anonymization	**:**	Making personal data unrelated to an identified or identifiable natural person under any circumstances, even by matching it with other data.
Employee(s):	**:**	Global Communities employees, subcontractor employees, subcontractor employees, interns
Employee PDP Policy	**:**	"Policy for the Protection and Processing of Personal Data of Global Communities Employees", in which the principles regarding the protection and processing of personal data of Global Communities employees are regulated.
Personal Data	**:**	Any information about an identified or identifiable natural person.
Personal Data Owner	**:**	Natural person whose personal data is processed.
Personal Data Protection Board	**:**	The unit that will provide the necessary coordination within the Association by the Global Communities within the scope of ensuring, retaining and maintaining compliance with personal data protection legislation.
Processing Personal Data	**:**	Provided that personal data are fully or partially automated or as part of any data recording system, any action taken on data such as obtaining, recording, storing, maintaining, modifying, rearranging, disclosing, transferring, taking over, making available, classifying or preventing its use by non-automated means.
PDPL	**:**	Law on the Protection of Personal Data No. 6698 dated March 24, 2016, published in the Official Gazette dated April 7, 2016 and numbered 29677.
PDP Board	**:**	Personal Data Protection Board
PDP Authority	**:**	Personal Data Protection Authority
Special Quality Personal Data	**:**	Data on race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, disguise, association foundation or union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data.
Global Communities /Association	**:**	Global Communities Inc. Turkey Representative Office
Global Communities Bussiness Partners	**:**	Parties to which Global Communities have partnered for various purposes while carrying out their activities
Global Communities Personal Data Retention and Destruction Policy	**:**	"Global Communities Personal Data Retention and Destruction Policy" in which the principles of personal data maintained by Global Communities are regulated.
Global Communities PDP Policy	**:**	Global Communities Personal Data Protection and Privacy Policy
Global Communities Suppliers	**:**	Parties that provide services to Global Communities on a contract basis.

Global Communities Data Owner Application Form	**:**	Application form to be used by data subjects when using their applications regarding their rights in article 11 of PDP.
The Constitution of the Republic of Turkey	**:**	The Constitution of the Republic of Turkey published in the Official Gazette dated 9 November 1982 and numbered 17863; No.2709 dated November 7, 1982
Turkish Penal Code	**:**	Turkish Penal Code No. 5237 dated 26 September 2004, published in the Official Gazette No. 25611 dated 12 October 2004.
Data Controller	**:**	It is the person who determines the purposes and means of processing personal data and manages the place where the data is kept systematically. It means the Global Communities Association in accordance with this Policy.