Personal Information Handling [Privacy] Policy

Revised on January 1st 2021

Enacted on January 1st 2020

GloZ Inc.

GloZ Inc. (“the company” hereinafter) operates and discloses the following Personal Information Handling Policy in order to handle user complaints efficiently while protecting the user’s personal information, rights and interests of the users pursuant to Article 30 of the Personal Information Protection Act.

In the event of an amendment to this Personal Information Handling Policy, the company will publicly notify the users thereof through an Announcement of GloZ (or notification by electronic means). The terms used in this Personal Information Handling Policy are defined to have identical meanings to those defined under the company’s Service Terms and Conditions.

Article 1 (Purpose of handling personal information)

The company handles the user’s personal information for the following purposes: Personal information handled by the company shall not be used for any purposes other than the purposes listed below, and the company shall take all necessary actions, including obtaining a new agreement pursuant to Article 18 of the Personal Information Protection Act, in the event of any change in the purposes:

1. Subscription to and management of membership

The company processes personal information in order to confirm the user’s intention to subscribe to the service, to identify the user for the provision of member-based services, to maintain and manage membership eligibility, to authenticate the user based on a limited user authentication system, to prevent the unauthorized use of the service, to post announcements and notices, and to handle complaints, etc.

(Minors below 14 years of age are not allowed to subscribe to this website.)

2. Integrated Membership Management

All GloHub Creator/GloHub Pro websites are joined, managed and unsubscribed as integrated members.

3. Service management

The company processes the user's personal information for the purpose of providing and managing the following services, forwarding contracts and invoices, providing contents and customized services, authenticating the user/age of the user, billing and payment, collecting accounts receivable, etc.

a. Provision of translation tools;

b. Provision of translation education and training;

c. Auto billing service

d. Payment service

4. Operation of the customer center

The company processes personal information for such purposes as authentication of civil petitioners, confirmation of petition related matters, contact, notices, notification of results of processing, etc.

5. Utilization for marketing and advertisement

The company processes personal information for the following purposes: development of new services (or products), provision of customized services, provision of information concerning events and ad messages, provision of information for participation opportunities, provision of services based on demographic characteristics, verification of validity of services, survey of access frequencies, statistical analysis concerning the use of the membership services, etc.

6. Taxation on use of service

The company processes personal information in order to generate data for tax returns, including invoices and tax bills issued based on the use of the service, and the withholding of income tax.

Article 2 (Items of personal information processed)

The company processes specific items of personal information for the following services:

1. Subscription to and management of membership, operation of the customer center, utilization for marketing and advertisement purposes

Translation requester:

Legal name in full, nickname, e-mail address,resident registration code, gender, resident country, and password

Company name and YouTube account

Service provider:

E-mail address, legal name in full, nickname, password, resident registration code, gender, resident country, preferences of genres, support roles, target and native languages, career information and education

Photo, recommender(s), schools graduated from, route of registration

2. Service management, taxation on use of the service

Translation requester:

Legal name in full, resident registration code, e-mail address, phone number, i-pin number, credit card number, bank account number and other payment information.

※ In the case of business operators, the information is collected by having the taxpayer registration certificate uploaded.

Particulars of past transactions, total no. of work hours

Service provider:

Legal name in full, resident registration code, e-mail address, phone number, i-pin number, bank account number and other payment information.

※ In the case of business operators, the information is collected by having the taxpayer registration certificate uploaded.

Particulars of past transactions, total no. of work hours

3. The company conducts tests to classify the level of the service providers and collects the following items of personal information:

Service provider:

E-mail address, Legal name in full

Education, qualifications/ certificates, language proficiency, experience, nationality, etc.

4. The following items of personal information may be generated and collected in the process of using the services provided by the company:

- IP address, cookies, service use history, records concerning visits and unauthorized or unlawful use, etc.

Article 3 (Processing and retention period of personal information)

(1) The company processes and retains personal information within the period for the retention and use of personal information provided under the relevant statutes or the period for the retention and use of personal information agreed to by the subject person at the time his or her personal information is collected.

(2) The periods for processing and retaining items of personal information are as follows:

1. Subscription to and management of membership, operation of the customer center, utilization for marketing and advertisement purposes: Until withdrawn

> However, personal information may be retained until the relevant reason for its retention is over in the following cases:

a. Until the investigation or probe of a violation of the relevant statues is completed;

b. Until the relevant debts or liabilities are settled when any remaining for the use of the site;

2. Service management, taxation on use of the service: Until the service provision, fee payment, or settlement is completed, or until the relevant period is over in any of the following cases:

a. Records concerning transactions, including labeling, advertisement, contract provisions and performance as provided under the Act on the Protection of Consumers in e-Commerce Transactions;

- Records concerning labeling. advertisement: 6 months

- Records concerning contract or subscription withdrawal, payment, and supply of goods: 5 years

- Records concerning consumer complaints and settlement of disputes: 3 years

b. Storage of data confirming communications-related facts pursuant to Article 41 of the Act on the Protection of Communications Secrets.

- Subscriber's telecommunications starting date, start and end times, counterpart subscriber number, frequency of use, originating base station, location tracing data: 1 year

- Computer communications, Internet log-on records, access point tracing data: 3 months

c. Records concerning e-financial transactions under the Electronic Financial Transaction Act: 5 years

d. Records concerning the Standards for Measures to Secure Personal Information Security

- Access authority data: 3 years

- Records of access to the personal information handling system: Varies depending on the number of personal information items (less than 5 million for 1 year, 5 million or more for 2 years)

3. Legal name in full, nickname, e-mail address, IP address, cookies, and records concerning unlawful use are retained for one year through technical measures under the related statute even after withdrawal in order to prevent reinstatement.

4. The records shall be retained or processed pursuant to the provisions of the relevant statute or regulations when the processing and retention periods are reset or modified based on the enactment of or amendment to the related statute.

(3) The company shall follow the personal information protection policy of the General Data Protection Regulation (GDPR) for residents of the European Economic Area (EEA).

Article 4 (Provision of personal information to third parties)

(1) The company shall process the personal information of the subject entities within the scope provided under Article 1 (Purposes of processing of personal information) and shall provide the personal information to third parties only in cases that fall under Article 17 of the Personal Information Protection Act or special statutory provisions, including when such processing and provision is consented to by the subject entity.

(2) The company provides personal information to third parties as follows:

Competent tax office and National Tax Service

Tax withholding, tax invoice

Resident registration code, paid amount, taxpayer registration code, legal name in full, business address

5 years

Customer centers

Actions, including customer counseling, refund, and difficulty in use inside sites

Legal name in full, nickname, e-mail address, resident registration code, gender, resident country, ID, password, working language, phone number, i-Pin number, payment information, including credit card number and bank account, details of past transactions, etc.

Article 3 shall be applied with any necessary modifications depending on types of customer complaints.

Article 5 (Outsourcing of processing of personal information)

(1) The company outsources the processing of personal information to third parties to efficiently perform the duties related to personal information as follows:

Outsourced duties and services:

Operation OF the Call Center

- Entrusted entity: GloZ INC. (US Corporation)

- Details of entrusted duties or services: Response for phone counseling, provision of information on departments and staff members, actions related to difficulties to access inside sites, etc.

- Outsourcing period: 5 years

(2) When an outsourcing contract is signed, the company supervises the safe processing of personal information by the outsourced entity pursuant to Article 25 of the Personal Information Protection Act by specifying the items concerning the responsibilities in the contract or other related documents, including the prohibition of personal information processing for purposes other than the performance of the outsourced duties, technical and administrative protective actions, restriction of subcontracting, control and supervision of the entrusted entity, and compensation of damages.

(3) The contents of the outsourced duties and the entrusted entity may be modified. In the event of any changes in the contents of the outsourced duties and the entrusted entity, the company will immediately announce the modified items without delay.

Article 6 (Methods of exercising rights and duties by information subjects)

The information subjects may exercise their rights in relation to the company and the protection of their personal information held by the company as provided under the following subparagraphs:

1. The information subjects may request to review their personal information;

2. The information subjects may request the correction of errors in their personal information, if any;

3. The information subjects may request to delete their personal information; and

4. The information subjects may request the discontinuance of the processing of their personal information.

(2) The information subject may exercise the rights provided under the foregoing paragraph 1 against the company in writing, by phone, e-mail, fax, etc., whereas the company shall take the appropriate actions without delay.

(3) When an information subject requests the correction or deletion of errors in their personal information, the company shall suspend its use or provision of the personal information until such errors have been corrected or deleted.

(4) The rights set forth in Paragraph 1 above may be exercised by the legal agent or person entrusted by the information subjects. In such a case, the applicant should submit a power of attorney.

(5) The rights of the information subject to request the review or discontinuance of the handling of his or her personal information may be restricted based on Article 35 paragraph 5 or Article 37 paragraph 2 of the Personal Information Protection Act.

(6) The information subject shall not request the correction or deletion of his or her personal information when it is clearly specified under other statutes that the personal information is subject to collection.

The company checks the identity of the information subjects and their agents to their legitimacy when they request to review, correct, delete, or discontinue the handling of their personal information according to their legal right.

Article 7 (Destruction of personal information files)

(1) The company shall immediately destroy the relevant personal information when it becomes unnecessary to retain it as the retention period has elapsed or the processing purpose has been achieved.

(2) When it is required to archive personal information based on other statutes although the retention period agreed to by the information subject has elapsed or the processing purpose has been achieved, the company shall transfer the relevant personal information to a separate database or store it in another location.

The company shall destroy personal information files by the following procedure and methods:

1. Procedure for destroying personal information files

The company shall destroy personal information files pursuant to the approval of its personal information protection manager after selecting the personal information files that need to be destroyed.

2. Method of destruction

The company shall destroy personal information recorded or stored in electronic files using a technical means that disables their recovery, and shall destroy personal information recorded or stored on paper documents by shredding using a document shredder or by incineration.

3. Destruction time limit

The user's personal information shall be destroyed within five days of the end date of the retention period when the retention period elapses, or five days from the day when it is deemed no longer necessary to handle the personal information when it is no longer required as the purposes of processing it have been achieved, abolition of the relevant service, or discontinuance of the service.

Article 8 (Measures for security of personal information)

The company takes the following measures to secure the safety of the user's personal information:

1. Administrative measures: Development, implementation, and periodic education of internal control plans, etc.

2. Technical measures: Control of access authority to personal information handling systems, etc., installation of access control systems, and installation of encryption or security programs.

3. Physical measures: Access control to computing rooms, data storage space, etc.

Article 9 (Information concerning the installation, operation or refusal of the device for collecting personal information automatically [cookies])

(1) The company saves the system access data and uses 'cookies' that fetch the access data as required in order to provide individually customized services to the users.

(2) Cookies are small bits of information which the server (http) used for operating the website sends to the user's computer browser and which are sometimes stored on the hard disc of the user's computer.

1. Purpose of using cookies: Cookies are used to provide the users with optimized information by surveying the frequency of their visits to services and websites and their patterns of use thereof, popular search words, secure access or not, etc.

2. Installation, operation or refusal of cookies: The users may refuse the storage of cookies on their computer by setting the relevant options on their web browser: Tools at top > Internet options > Personal Information Menu.

3. If they refuse the storage of cookies, they may experience difficulties in using the customized service.

Article 10 (Personal information protection manager)

(1) The company appoints a personal information protection manager to address user complaints related to the handling of their personal information etc. to remedy damages, and to assume overall supervision of the company's operations related to the processing of personal information:

▶ Personal information protection manager

- Legal name in full: Kug Koung Lee

- Position: CEO

- Contact phone number: < Phone No.> +82-70-8667-1191

<E-mail address> info@GloZinc.com

<Fax number> +82 303-3442-5581

▶ Department in charge responsible for the protection of personal information

- Name of department: Development team

- Person in charge: Hokyun Kim

- Contact phone number: < Phone No.> +82-70-8667-1191

<E-mail address> info@GloZinc.com

<Fax number> +82 303-3442-5581

※ You will be connected to the personal information protection department.

(2) The information subjects may ask the personal information protection manager or the responsible department any questions concerning the protection of their personal information, the handling of complaints, and remedies of damages arising while using the service, and the company will respond to or handle such questions without delay.

Article 11 (Request for review of personal information)

The information subjects may request the following department to review their personal information based on Article 35 of the Personal Information Protection Act: The company will do its best to ensure such review requests are processed rapidly.

▶ Department that accepts and handles request for reviews of personal information

- Name of department: Development team

- Person in charge: Hokyun Kim

- Contact phone number: < Phone No.> +82-70-8667-1191

<E-mail address> [info@GloZinc.com]

<Fax number> +82 303-3442-5581

Article 12 (Redress of infringement of rights or interests)

The information subjects may ask the following agencies about redress and counseling regarding infringements of personal information:

<As the following agencies are separate from the company, you may contact them for help or further information if you are dissatisfied with the company's handling of complaints concerning personal information or any redress or actions taken regarding damages.>

▶ Personal Information Infringement Report Center (operated by KISA)

- Duties: Acceptance of reports and counseling on infringements of personal information

- Website: privacy.kisa.or.kr

- Phone: 118 (without area or station code)

- Address: Personal Information Infringement Report Center (58324) 3rd floor, 9 Jinheung-gil, Naju-si, Jeollanam-do (301-2, Bitgaram-dong)

▶ Personal Information Dispute Mediation Committee

- Duties: Acceptance of requests for personal information dispute mediation, mediation of collective disputes (civil settlement)

- Website: www.kopico.go.kr

- Phone: 1833-6972 (without area or station code)

- Address: (03171) 4th floor, Central Government Complex, 209 Sejong-daero, Jongno-gu, Seoul

▶ Supreme Prosecution Service Cyber Crime Investigation Group: 02-3480-3573

▶ Cyber Security Bureau, National Police Administration 182

Article 13 (Change of personal information handling policy)

① This personal information processing policy shall enter into force on January 1, 2020.

Supplementary Rules

Article 1 (Efforts for compliance with GDPR)

GloZ Inc. ("the company" hereinafter) shall comply with the EU General Data Protection Regulation (GDPR) as follows:

- It shall carry out activities aimed at enhancing awareness of the GDPR;

- It shall assess the impact test on personal information;

- It shall guarantee the rights of the users of its services; and

- It shall report and notify the users of leakages of their personal information.

Article 2 (Efforts for enhancing awareness of GDPR)

The company makes enterprise-wide efforts to comply with the GDPR. The company does its best to comply with the GDPR through the following activities while checking the influence GDPR may have on this organization:

- Participating departments: Customer Service, HR, Finance, System Development, etc.

- Questionnaire survey of the level of constituents' knowledge concerning the protection of personal information.

- Official declaration of the management's determination to follow the GDPR.

- Encouragement of participation in the GDPR conference and seminars.

- Management of checklists of items to be performed by the department.

Article 3 (Assessment of impact on personal information)

The company assesses the impact of the following on personal information in the following cases that may pose a high risk to the rights and freedoms of natural persons as defined under the GDPR:

1. Assessment or scores;

2. Automatic decision making with legal effect or other similar effect;

3. Audit using systems;

4. Sensitive information;

5. Information processed in large volumes;

6. A group of information that is interconnected or combined;

7. Information concerning vulnerable data subjects.

Article 4 (Guarantee of users' rights)

The company makes efforts to guarantee the following user rights as defined under the GDPR:

- The right to delete one's personal information (the right to be forgotten);

The data subjects have the right (to delete), by which they can demand the deletion of their personal information.

1. When it is no longer necessary for the purpose of the collection or processing of personal information;

2. When the data subject has withdrawn their consent to the processing of their personal information and there exists no legal basis for retaining and processing such personal information;

3. When the data subjects oppose the processing of their personal information based on Article 21 (Right to object) of the GDPR, when there exists no justifiable cause overriding the processing of the relevant personal information, or when the information subjects object to direct marketing under Article 21 paragraph 2 of the GDPR;

4. When personal information is processed illegally;

5. When the deletion of personal information is required to comply with the statutes of the EU or its member countries; and

6. When personal information is collected in connection with the provision of information societal services for children.

However, GloZ may refuse requests for the deletion or personal information in cases falling under any of the following:

1. When it is necessary for the due exercise of rights related to expression and information;

2. When it is necessary to comply with the legal obligations of the EU and its member countries, to provide services in the public interest, or to exercise the official authority vested in GloZ;

3. When it is necessary for public health purposes;

4. When it is necessary for public records archival, scientific or historic research, and statistics; and

5. When it is necessary for proving, exercising, or defending legal claims.

- Right to data portability

1. When the data subject requests, the company shall provide him/her with information without undue delay. The company shall provide the information concerning data portability taken by the company within one month from the receipt of the request for data portability. When it takes time as the requested information is complicated, the company shall notify the data subject of the reason for the extension and the length of the extended period (an extension of two months is allowed, but a maximum of three months may be required) within one month.

2. If the company fails to take action to meet the data subject's request, the data subject may request the company to provide the reason for its failure to take action within one month without delay, and may seek legal redress through a supervising agency.

3. The data portability service is provided free of charge.

4. The data subject may have the personal data transmitted directly from one controller to another, where technically feasible.

5. When the company receives a request from a data subject for data portability of the personal data, the company shall provide the portable data "in a structured, commonly used and machine-readable format".

Article 5 (Report and notification of personal information leakage)

(1) In the event that any of the following infringements threaten the rights and freedoms of individuals, the company shall report the facts to the supervising authorities within 72 hours of its discovery of the leakage:

1. Discriminatory acts;

2. Defamation;

3. Financial loss;

4. Leakage of secrets;

5. Risks related to other crucial economic or societal disadvantages.

(2) When a leakage is expected to pose a high risk to the freedoms and rights of the data subjects, the company shall notify them thereof without delay.

Article 6 (Enforcement Date)

The amendments to this privacy policy will be effective from January 01, 2021.