Privacy Policy

Fitogether Inc., (hereinafter referred to as the "Company") establishes and presents the following privacy policy in order to protect the personal information of the users who use the Company's services and resolve any relevant complaint.

1. Purpose of Processing Personal Information

1.1 The Company collects and uses personal information for the following purposes.

(a) Provision of goods or services: delivery of goods, provision of general/custom services, delivery of contract/invoice, verification of identity, age verification, bill payment and settlement, debt collection, etc.

(b) Managing user complaints: identification of the user, confirmation of complaints, contact/notification for fact-finding, and notification of processing results

(c) Marketing and Advertising: provision of customized advertisements, opportunities to participate in events, provision of information regarding events

(d) Service Improvements and Development: improvement of existing services and development of new and customized services

(e) Utilization of Pseudonymized Information: pseudonymizing, processing and use of pseudonymized information for statistical preparation, scientific research, and preservation of records in the public interest.

2. Items of Personal Information Processed

2.1 The Company collects and processes the following personal information of service users.

(a) Information collected during serving inquiries: name, email, address, position within the team, team name, team nationality, team age group, team gender

(b) Information collected when using paid service

(i) When paying by credit card: credit card information such as the name of the card company and card number

(ii) In case of bank transfer: bank account information such as the name of the account holder, account number, and bank holding the account

(iii) When paying by mobile phone number: payment information such as phone number and telecommunication company

(c) When using the service, the following personal information items are collected automatically: access country

(d) For managing user complaints: collects and processes necessary information among the above and other necessary information required to resolve the complaints from the user

3. Period of Retention and Use for Personal Information

3.1 The Company will, without delay, delete and destroy the user's personal information when it achieves the purpose of collection and use of personal information. In the above cases, the personal information shall be deleted or destroyed regardless of the user's request. Nevertheless, the following personal information is retained for reasons stated below:

(a) If there is an ongoing investigation regarding a violation of relevant laws and regulations, the personal information shall be retained until the completion of the respective investigation

(b) If any debts or debt relationship pursuant to the use of the services remain unsettled, the personal information shall be retained until the relevant debts are settled

(c) If the Company terminates the service use contract according to the Terms of Use, any records of the illegal use of the Services shall be retained for one (1) year to prevent any unauthorized re-registration and use of service.

3.2 Notwithstanding the foregoing, the following information is retained for the period specified for the reasons stated below:

(a) Personal information related to use of service (log records): 3 months (Communications Secret Protection Act)

(b) Records on withdrawal of contract or subscription, etc., and records on payment and supply of goods: 5 years (Consumer Protection Act in Electronic Commerce, Etc.)

(c) Records on handling consumer complaints or disputes: 3 years (Consumer Protection Act in Electronic Commerce, Etc.)

(d) Books and evidentiary documents for all transactions prescribed by tax laws: 5 years (Framework Act on National Taxes)

3.3 The Company shall separately store or delete personal information of users who have not used the service for a period of one (1) year or any other period set forth by the user.

4. Provision of Personal Information to Third Parties

4.1 The Company may provide personal information to third parties only with the consent of the user or when there are special provisions in the Personal Information Protection Act or other laws.

5. Processing Personal Information Subsequent to Outsourcing of Work and Overseas Transfer

5.1 The Company entrusts the following personal information processing tasks for smooth personal information processing.

Trust Companies (Consignee)	**Outsourced Work**
Amazon Web Service, Inc.	Sending emails

6. Use and Provision of Personal Information within the Scope Reasonably Related to the Purpose of Collection

6.1 The Company may use or provide personal information to a third party without the consent of the user, considering each of the following criteria within a reasonable scope and the original purpose of collection.

(a) Whether or not it is related to the original purpose of collection: judgment based on whether the original purpose of collection and the purpose of additional use and provision are related in terms of their nature or tendency;

(b) Whether or not the further use or provision of personal information is predictable considering the circumstances in which the personal information was collected or the processing practices: judgment based on the relationship between the personal information controller and the user, the level of technology and the rate of development, and general circumstances (practice) established over a substantial amount of time, etc.;

(c) Whether the interests of the user are unreasonably infringed: judgment based on whether the interests of the user are substantially infringed in relation to the additional purpose of use and whether the infringement of the interests is unreasonable, etc.; and

(d) Whether measures necessary to secure safety, such as pseudonymization or encryption, have been taken: judgment by considering whether safety measures are taken in consideration of the possibility of infringement, etc.

7. User's and Legal Representatives' Rights and Methods for Exercising the Rights

7.1 The user can exercise the right to read, correct, delete and suspend processing his or her personal information against the Company at any time.

7.2 The exercise of the rights pursuant to Section 7.1 can be made to the Company in writing, by phone, or by e-mail, and the Company will take action without delay.

7.3 The exercise of rights pursuant to Section 7.1 may be done through an agent such as a legal representative of the user or a person who has been delegated. In this case, a power of attorney must be submitted to the Company that confirm such delegation.

7.4 In accordance with relevant laws such as the Personal Information Protection Act,

the exercise of the user's right to access, correct, delete, or suspend the processing of personal information may be restricted.

7.5 Request for correction and deletion of personal information cannot be requested if the information is required to be collected according to other laws.

7.6 The Company shall confirm whether the person who made the request, such as a request for reading, correction, or deletion, or request for suspension of processing, holds such right or is a legitimate agent.

8. Destruction of Personal Information

8.1 The Company destroys the personal information without delay when the personal information becomes unnecessary, such as in the cases of the expiration of the personal information retention period, or achievement of the purpose of processing.

8.2 If personal information needs to be preserved in accordance with the laws and regulations even when the personal information retention period agreed by the user has elapsed or the purpose of processing has been achieved, the personal information will be moved to a different place or stored in a separate database (DB).

8.3 The destruction procedures and methods are as follows:

(a) Destruction procedures: The Company selects the personal information that needs to be destroyed and destroys the personal information with the approval of the Company's personnel for management of personal information.

(b) Destruction method: The Company destroys personal information recorded and stored in electronic file format using technical methods so that the information cannot be reproduced, and personal information recorded and stored on paper documents is destroyed by crushing or incineration with a shredder.

9. Measures to Ensure Safety of Personal Information

9.1 Company is taking the following measures to ensure the safety of personal information

(a) Administrative measures: establishment and implementation of internal management plans for personal information, regular employee training, etc.

(b) Technical measures: technical countermeasures against password hackings, etc., encryption of personal data, storage access records, and prevention of forgery, etc.

(c) Physical measures: Access control to server rooms, data storage rooms, etc.

10. Installation, Operation, and Rejection of Automatic Personal Information Collection Devices

10.1 The Company may use 'cookies' to store and frequently retrieve usage information to provide users with individually customized services. Cookies are a small amount of information sent to the user's PC browser by the server (HTTP), which are used to operate the website, etc., and are also stored in the user's hard disk in the

computer.

(a) Purpose of using cookies: security management and improving services, developing new services, and providing customized services and advertisements by analyzing access frequency and access time of users, etc., identifying the patterns of service usage and tracking traces, secure access status, and the number of users.

(b) Installation, operation, and rejection of cookies: Users have right to choose the installation of cookies. Therefore, the users may refuse to save all cookies by changing their Internet browser options.

(c) However, if you refuse to store cookies, it may be difficult to use some services of Company.

11. International Transfer of Personal Information

11.1 The Company may store, process, and transmit personal information in the Republic of Korea or other locations outside the European Economic Area ("EEA"). Data may also be stored locally on the devices user uses to access the service. When the Company transfers personal information outside the EEA or the Republic of Korea, the Company will ensure that a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

(a) The Company will only transfer personal information to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.

(b) Where the Company uses certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe.

12. Rights Protected under the General Data Protection Regulation (GDPR)

12.1 If the user is an individual located in the European Economic Area ("EEA") or the United Kingdom ("UK", the General Data Protection Regulation ("GDPR") and the UK-GDPR, respectively, grant additional privacy rights and protection. These include the following rights:

(a) right to be informed about processing activities and applicable rights;

(b) right to access data or obtain data being processed;

(c) right to rectify information when outdated or incorrect;

(d) right to delete information and to be publicly forgotten;

(e) right to object to processing and particularize consent based on activity;

(f) right to restrict processing when processing is deemed to be unlawful;

(g) right to data portability between proprietary systems in a common format; and

(h) rights related to automated decision making, including decisions based on profiling activities.

12.2 Such requests and exercise of rights or any inquiries regarding data protection matters under the GDPR (or UK-GDPR respectively) may be initiated or requested by contacting the Company's Personal Information Manager in Section 13.1 or its representative in the EEA (or UK) pursuant to Article 27 of the GDPR (or UK-GDPR). VeraSafe has been appointed as Fitogether's representative in both the EEA and the UK for data protection matters.

12.3 If you are in the European Economic Area and you wish to contact VeraSafe for the processing of your personal data, please contact VeraSafe using this contact form: https://verasafe.com/public-resources/contact-data-protection-representative or telephone at: +420 228 881 031.

12.4 If you are in the United Kingdom and you wish to contact VeraSafe for any the processing of your personal data, please contact VeraSafe using this contact form: https://verasafe.com/public-resources/contact-data-protection-representative or telephone at: +44 (20) 4532 2003.

12.5 The Company may take reasonable steps to verify the user's request and will fulfill the requests to the extent the request does not violate applicable law and/or the information is not essential for billing, fraud prevention or security purposes. In the event the Company denies the user's request, the Company shall provide the reason(s) for denying the user's request.

13. Personnel for Management of Personal Information

13.1 The Company has designated the person in charge of personal information management and handling complaints about personal information, and the contact information is as follows.

Personal Information Manager		
	Name:	Sueyoung Oh
	Title:	Director
	Telephone No.:	+82-(0)2-6263-8930
	Email Address:	privacy@fitogether.com

13.2 The user can inquire about all personal information protection-related inquiries, handling complaints, damage relief, etc. that occurred while using the Company's service (or business) to the person in charge of personal information protection and the following department in charge.

	Department Name:	Risk Management Team
	Telephone No.:	+82-(0)2-6263-8930
	Email Address:	privacy@fitogether.com

14. Amendment of the Privacy Policy

14.1 The Company may amend the Privacy Policy in order to comply with applicable law or to reflect any changes in the provision of service. In the event this Privacy Policy is amended, the Company shall notify the users in advance through a notice on the website at least 7 days prior to the amendment. The amended Privacy Policy shall take effect from the Effective Date stipulated in the Amendment. However, the Company shall notify the users at least 30 days in advance for any major changes in the Privacy Policy, such as the items of personal information to be collected or the rights of the users.

The Privacy Policy shall take effect from [January 01, 2022].