Privacy Policy

The Soder Code (hereinafter referred to as the 'Company') collects minimum personal information when necessary, and the personal information collected is used only within the scope of notification and consent from the customer. The company does not use or disclose to the public beyond the scope of the contents agreed in advance.

However, if there is a regulation in the law or if the investigative agency or the administrative agency requests it with the court's permission, the minimum information may be provided without consent through internal procedures. In addition, the company is doing its best to protect the rights and interests of users by establishing a personal information processing policy to safely process their personal information. The company will notify users in advance if there is an amendment to the personal information processing policy and post it through a notice so that users can check it.

The Soder Code Privacy Policy includes the following.

1. Purpose of collecting and using personal information
2. Providing third-party personal information
3. Consignment of personal information processing
4. The rights of users and legal representatives and the method of exercise thereof
5. Personal information destruction procedures and methods
6. Technical and management protection measures for personal information
7. Matters concerning the installation, operation, and refusal of an automatic collection device for personal information;
8. Managing smartphone apps
9. The obligation of users (members
10. The person in charge of personal information protection and the department in charge of handling civil petitions
11. Reporting and consulting privacy violations
12. Other points
13. Duties of notice

1. Article 1 (Personal Information Collection and Use Purpose)

1. Personal information collected step by step

The company collects and uses the minimum personal information after agreeing with you.

Sortation	Collection point	category	Collection method	Purpose of use	Retention and Use Period
Required Information	When logging in with your social ID	Facebook login generation number, Google login generation number	Online	Subscription, service use and counseling, fraudulent use identification and prevention	

2. Member information collected and used by other statutes

Retention information	Retention period	A legal base
Records of payment and supply of goods, etc.	5 years	Act on the Protection of Consumers in Electronic Commerce, etc.
Records of contract or subscription withdrawal, etc.	5 years	Act on the Protection of Consumers in Electronic Commerce, etc.
Records of handling consumer complaints or disputes	3 years	
Records of display and advertising	5 months	
Web Site Visit History	3 months	the Communications Secrets Act

3. Marketing and advertisement utilization

If the company needs to use your information for marketing, it is getting a separate consent in advance.

2. Article 2 (Personal Information Processing Consignment)

1. In order to provide better service to users, the company may be entrusted with some of its business affairs.
2. The company requires the trustee to comply with the information protection regulations through documents such as contracts when entrusting personal information processing.
3. When the company entrusts personal information processing, it reflects the contents of the contract so that the contracted trust company meets the standards for safety-guaranteed measures required by the Act on Personal Information Protection.
4. The company requires the trustee to take technical and administrative protective measures to safely handle your personal information, such as safe processing of personal information, access or access records, restriction of use, and encryption.
5. The details of business and business of the company processing and entrusting personal information are as follows.

Sortation	an entrusted company	Contents of consignment work	Retention and Use Period
Payment	Paypal	Domestic and overseas payment agencies	Upon membership withdrawal or until the end of the service (handled only if the user uses the service)

3. Article 3 (User's rights and methods of exercise)

6. Users can inquire or modify their personal information at any time and withdraw their personal information through the withdrawal process.
7. If you want to modify your personal information or wish to withdraw from the membership, you can proceed with the following procedure.
8. Users can request modifications, deletions, or withdrawals through 070-4077-0327 or help@sothecode.com. However, we can inform you that business procedures may be required to clearly confirm that the information subject to the request is you, and that you must submit them through the standard form separately provided by the Ministry of Public Administration and Security to handle the work.
9. 3) If the user wants to leave the service, he/she can leave the service through the security verification process by clicking [Exit] on the [Settings] menu.
10. Even if a user requests a right to modify, delete, or withdraw personal information, this right request may not immediately apply to a member who is subject to the company's policy of suspension of service for reasons attributable to the user.
11. Even if a user requests the withdrawal, deletion, or suspension of processing of consent, the expiration date under compliance with the statute may be applied first if it must be collected or preserved in accordance with other statutes.
12. Users can join membership only if they are 14 years old or older. In principle, personal information of children under the age of 14 is not collected. Children under the age of 14 need the consent of their legal representatives.

4. Article 4 (Procedures and methods for destroying personal information)

13.1. The company immediately destroys the user's personal information if it is necessary to destroy the user's personal information after achieving the business purpose or holding period. However, information that must be kept under other laws and regulations is subject to a certain period of time as prescribed by the Act.

14. Personal information destruction procedures, methods, and dormant conversion policies are as follows.

15. Destruction Procedure and Method

16.1) If the purpose of collecting and using the user's personal information is achieved, it will be destroyed without delay. Personal information printed on paper is destroyed by shredder or incineration, and personal information stored in an electronic file format is deleted using technical methods that cannot be played back.

17.2 Notwithstanding the destruction regulations of the Information and Communication Network Act, personal information that must be preserved under other statutes shall be safely stored in a separate database for a certain period of time to comply with the relevant statutes and internal regulations.

18. Restoration Policy (Personal Information Validity System)

19.1) The company informs users of the plan to take a rest 30 days before the time of transition to sleep for users (sleeping members) who have no service records for a year.

20.2) After one year of sleepover guidance, the information of dormant members is transferred to a separate DB and stored separately. However, if there is a period designated by the user when signing up, the period requested by the user will be applied.

21.33) If a dormant user requests the use of the service, the personal information may be restored again when the service is resumed.

22.4) The personal information of a user stored separately shall be destroyed without delay upon the expiration of a certain period specified in the relevant statutes.

5. Article 5 (Technical/Management Protection Measures for Personal Information)

The company is preparing the following technical/management protection measures to ensure safety so that personal information is not lost, stolen, leaked, tampered with, or damaged when processing user personal information.

1. Organizing an information security professional organization
1) The company operates a team that carries out technical and management protection measures for personal information in order to protect the users' personal information safely.

2. Encrypting personal information
1) The user password is stored and managed in a one-way encryption, and only you yourself can know the password. Therefore, please be careful not to let others know your password.
2) The company is performing the encryption required by the statute. Financial information, such as account number, is stored and managed in accordance with the algorithms required by law.
3) The company encrypts the user's personal information transmission section, and encrypts important data or sets the password on the file when performing business in-house.

3. Countermeasures against hacking, etc.
1) The company is doing its best to prevent personal information from being leaked or damaged by hacking or computer viruses.
2) The company continues to make efforts to secure technological protection to ensure better security measures.
3) The company controls unauthorized access from the outside and strives to have all possible technical devices to ensure system security.

4. Minimize personal information handlers and continue training
1) The company minimizes the number of employees who handle personal information, and conducts training for related employees from time to time to check whether they are in compliance with this policy.
2) The person handling personal information is reviewing whether the authority is appropriate and is taking measures to ensure that minimum authority is granted.
3) The company regularly updates the password of the personal information handler's account.

4) The medical institution continuously emphasizes the obligations of compliance with laws and regulations related to personal information protection and policies for personal information processing through regular and occasional education for personal information handlers.

6. Article 6 (Information on the installation/operation and rejection of automatic personal information collection devices)

1. What is a cookie?

1) In order to provide personalized and customized services, the company uses 'cookie' that stores user information and retrieves it from time to time.

2) Cookies are very small text files sent to the user's browser by the server used to run the website and are stored on the user's computer's hard disk.

3) When a user visits a website, the website server is used to maintain user preferences and provide customized services by reading the contents of cookies stored on the user's hard disk.

4) Cookies do not automatically or actively collect information identifying individuals, and users may refuse or delete such cookies at any time.

5) It is used to provide customized information that is optimized for users by identifying the types of visits and use of services and websites visited by users, search terms, and security access.

2. Installing/operating and rejecting cookies

1) The user has the option of installing cookies. By setting options in your web browser, you can also allow all cookies, go through a confirmation whenever a cookie is saved, or refuse to save all cookies. However, if you refuse to store cookies, some services that require login may be difficult to use.

2) Here's how to specify whether to allow cookies to be installed in Internet Explorer:

A. From the Tools menu, select Internet Options.

B. Click the Privacy tab.

C. You can set the [Personal Information Processing Level].

7. Article 7 (Smartphone App Management)

1. If it is necessary to access information on the device when using the service through the smartphone app, notify it and obtain approval.
2. If you change your permission to access the smartphone app, you can change it on your smartphone under Settings > Application Manager. For more information, see the smartphone app store.

8. Article 8 (Duties of Users (Members))

1. Users are obliged to comply with the Personal Information Protection Act, such as the Promotion of Information and Communication Network Use and Information Protection Act, and the Personal Information Protection Act, in order to keep their personal information safe.
2. Users are obliged to protect their personal information safely, and the company is not responsible for what has happened due to the carelessness of the customer. Therefore, you are obliged to do your best to protect your personal information, such as thoroughly managing your ID and password and periodically changing them.
3. Users are obliged to enter and maintain their personal information accurately and up-to-date. You are responsible for any problems caused by your inaccurate input of information.
4. Users may be punished according to the Personal Information Act, along with the loss of membership status, if they use other people's personal information.
5. Users also have an obligation not to violate or disclose personal information about others. Any person who mentions or leaks personal information he or she has learned about other members while using the service may be punished according to the privacy law.

9. Article 9 (Personal Information Protection Officer and Civil Service Disposal Department)

1. Person in charge of personal information protection
- Name: Kim Hyun Young
- Position: Senior Researcher
- Position: Head of development team
- Contact: sothecode@sothecode.com / 070-4077-0327

2. Department in charge of handling personal information complaints
- Department name: Customer center
- Contact: sothecode@sothecode.com / 070-4077-0327

You can contact the person in charge of personal information protection, complaint handling, damage relief, etc. using the service provided by the company, and the company will provide sufficient answers to the users' reports and inquiries.

10. Article 10 (Report and consult on privacy violations)

If you need to report or consult on other privacy violations, please contact the following institutions:

- Personal Information Dispute Mediation Committee (www.kopico.go.kr / Telephone 1833-6972)
- Personal Information Infringement Reporting Center (privacy.kisa.or.kr / No National Number 118)
- Cyber Crime Investigation Team of the Supreme Prosecutors' Office (www.spo.go.kr / 02-3480-3571)
- Cyber Security Bureau of the National Police Agency (cyberbureau.police.go.kr / No National Number 182)

11. Article 11 (Duties of Notice)

This privacy policy will be applied from the date of enforcement, and if there is any addition, deletion, or correction of changes under statutes or policies, we will notify you through the notice seven days before the change takes effect. Also, if we need to change the processing policy due to changes in related laws or company policies, we will notify you quickly through the website notice, so please refer to it.

Notice date: March 1, 2020
Date of implementation: March 1, 2020