







NAVER Cloud Platform - Privacy Policy

NAVER Cloud Corporation (hereinafter the "Company") complies with the privacy regulations of applicable laws that must be observed by information and communication service providers, such as the Personal Information Protection Act, the Act on Promotion of Information and Communication Network Utilization and Information Protection, Etc., the Protection of Communications Secrets Act, and the Telecommunications Business Act. The Company establishes this privacy policy based on these laws and makes its best efforts to protect the rights of its customers. This privacy policy is applicable to the services provided by the Company and covers the following:

[Key personal information processing labels]

The Company's key personal information processing activities can be summarized as follows. Details can be found in the main text of the Privacy Policy.

		
<p>General collection of personal information</p>	<p>Purpose of processing personal information</p>	<p>Personal information retention period</p>
<p>- Membership sign-up 1. For individual member sign-ups: email address, password, name, mobile phone number, country of residence 2. For business member sign-ups: email address, password, company name, name of person in charge, mobile phone number, country of residence</p> <p>※ See the full Privacy Policy for details.</p>	<p>- Membership sign-up and management - Contractual fulfillment and settlement of fees for the provision of services - Development of new services and utilization in marketing advertising</p>	<p>- Prompt destruction upon the Customer withdraws from the membership or the purpose for its use has been satisfied. - Additional retention based on separate consent from the information subject - Retention for up to 5 years based on relevant laws, etc.</p>
		
<p>Provision of personal information</p>	<p>Processing consignment</p>	<p>Privacy complaint department</p>
<p>- LINE WORKS Corp, NAVER Cloud Platform partners, etc.</p> <p>※ See the full Privacy Policy for details.</p>	<p>- NAVER, NAVER FINANCIAL, etc.</p> <p>※ See the full Privacy Policy for details.</p>	<p>- Security Policy&Privacy - +82-1544-5876 - dl_ncloud_privacy@navercorp.com</p>

Chapter 1 Personal Information Processing Purpose, Retention Period, and Collection Items

Article 1 (Purpose of Processing Personal Information)

We process personal information for the following purposes. The personal information processed won't be used for any purpose other than the following, and if the purpose of use changes, we will take necessary measures such as obtaining separate consent in accordance with Article 18 of the Personal Information Protection Act.

1. Membership sign-up and management

The Company collects personal information for member management purposes to verify user identities for using member services, to confirm individual identification, to prevent illegal use and unauthorized use by inadequate members, to confirm account registrations, to prevent duplicate registrations, to validate identities of legal representatives, to archive records for dispute resolution, to process civil complaints, to provide notices, and to confirm member's decision to withdraw membership.

2. Execute service agreements and process transactions related to service offerings

The Company collects personal information to provide Customers with content and customized services, deliver goods, issue invoices, verify user identities, process purchases and fee payments, and collect fees.

3. New service development and utilization in marketing advertising

The Company collects personal information for the purposes of developing new services and customizing services, providing existing services and posting advertisements based on user demographics, validating services, providing event information and advertisements as well as opportunities for Customer participation, understanding Customer access frequency, and developing statistics on Customer use of services.

Article 2 (Processing and Retention of Personal Information)

In principle, the Company will destroy, without delay, the Customer's personal information once the Customer withdraws from the membership or the purpose for its use has been satisfied. However, the following information will be retained for a specified period due to reasons stated below:

1. When separate consent is obtained for the personal information retention period

Retained Information	Reason for Retention	Retention Period
Records of illegal use	Prevention of illegal use	1 year after membership withdrawal
Inquiry details (If additional consent has been obtained from the customer)	Customer consultation processing	3 years
Attachments determined to be infected malicious files	Analysis of the malicious files	1 month
Required documents for copyright infringement or harmful post reports	Processing reports	3 months

Retained Information	Reason for Retention	Retention Period
Information generated from NAVER WORKS, WORKBOX, GAMEPOT, and Ncloud Chat	User protection purposes such as data recovery requests	7 days from the request date of service cancellation
Recording violations of the Occupational Safety and Health Act	Preventive measures and sanctions for health damage caused by customer's abusive language, etc.	3 years
Required documents of Duplicate payment cancellation processing	Response to regulatory requests, including tax audits	Retained for 6 years and 3 months from the last transaction date
Training and event request information	Training and event management	3 months

2. Retention of information due to related laws and regulations

The Company retains members' information for a specific period in accordance with applicable laws and regulations, including the Commercial Act and the Act on the Consumer Protection in Electronic Commerce, Etc. In this case, the Company will only use the retained information for the purpose of its retention. The retention periods are as follows:

Retained Information	Reason for Retention	Retention Period
Contract or subscription withdrawal records	Act on the Consumer Protection in Electronic Commerce, Etc.	5 years
Records on payment or supply of goods and others		5 years
Customer complaints or dispute handling records		3 years
Display/advertisement records		6 months
Ledgers and evidentiary documents of all transactions under the tax laws	Framework Act on National Taxes, Corporate, Value-Added Tax Act	5 years
Electronic transaction history	Electronic Financial Transactions Act	5 years
Copyright infringement history	Copyright Act	1 year
Login records	Protection of Communications Secrets Act	3 months

3. Retention of information due to internal policies

Retained Information	Reason for Retention	Retention Period
email address verified during membership registration process	email authentication and customer service processing	2 months

Article 3 (Personal Information Items to be Processed and Collection Methods)

- ① The company minimally collects the following required personal information for creating accounts, providing customer consultation, and allowing customers to access and use various services:
1. Membership sign-up and management
 - 가) For individual member sign-ups
 - Required information: email address, password, name, mobile phone number, address, country of residence
 - 나) For business member sign-ups
 - Required information: email address, password, company name, name of personal information, mobile phone number, address, country of residence
 - 다) Log in with NAVER ID
 - Required information: name, mobile phone number, email address
 2. Settlement of fees based on service provision
 - 가) For registering automatic payment methods
 - Credit card: date of birth (business registration number for businesses), card number, expiration date
 - Bank transfer (For the Korean corporate members): bank name, date of birth (business registration number for businesses), account number
 - Documents related to business (For Korean corporate members): Business representative name, business registration number, and a copy of business registration certificate
- ② The following information may automatically be created or additionally collected during service use or processing of service provision tasks:
- IP address, cookies, device information, access logs, date of visit, service use records, bad use records, payment records
- ③ The following additional information may be collected from the customers of certain services during the process of service use.

1. In cases for which separate consent for the collection of personal information has been obtained

Type	Collected Personal Information Items
General inquiries	- Required: email address, mobile phone number
Sales inquiries	- Required: email address, mobile phone number, company name - Optional: name

Cash receipt requests	- Required: mobile phone number or cash receipt card number/ (For businesses) business registration number
Receive Advertising Information	- Required: name, email address, mobile phone number
Newsletter subscription requests	- Required: name and email address, country of residence - Optional: affiliation and company name
Marketplace solution subscription	- Required: name, email address, mobile phone number
Copyright infringement or harmful post reports	- Required: name, email address, mobile phone number, and required documents (Copy of ID (items other than name and date of birth are masked))
Change of member's basic information	<Verification of contract subject change request> 1) Individual member - Required: personal seal certificate of the requestor 2) Business member - Required: corporate seal certificate or proof of employment of the requestor
Duplicate payment cancellation request	1) Individual member - Required: account number, Copy of ID (items other than name and date of birth are masked) 2) Business member - Required: corporate seal certificate, account number, manager name, mobile phone number, email address
Request for training and events	- Required: name, company name, email address, mobile phone number, company name, duty - Optional: affiliated department, job title

Service	Collected personal information items
User environment diagnostics tool	<Measurement of service quality> - Required: client IP
Simple & Easy Notification Service	<Identity verification for customers who fail SMS verification for caller ID registration>

	<p>1) Telecom service proof of use - Required: telecom company name, name, address, date of birth (business registration number for corporate member), phone number</p> <p>2) Power of attorney - Required: name, business registration number, address, mobile phone number</p> <p>3) Proof of employment - Required: name, affiliation, years of service</p> <p><Biz Message service subscription></p> <p>1) Individual member - Required: Copy of ID (items other than name and date of birth are masked), Kakao ID verified on the Kakao Talk channel</p> <p>2) Business member - Required: business registration certificate, information of person in charge (name, email address, mobile phone number, proof of employment), Kakao ID verified on the Kakao Talk channel</p>
Cloud Security Watcher	<p><Service subscription> - Required: admin ID, name, email address, IP, password</p> <p><Account Link> - Required: account name, API Key, name, email address</p>
Cloud Data Box	<p><Service subscription> - Required: username, password, mobile phone number, email address</p>
Data Box Frame	<p><Service subscription> - Required: username, password, mobile phone number, email address</p>
Data Catalog	<p><Service subscription> - Required: ID, password</p>
Data Query	<p><Service subscription> - Required: ID, password, API Key</p>
NAVER WORKS	<p><Service subscription> - Required: admin ID, password, company name <Sending location and specifying location for schedule> - Optional: location information <WORKS Finance - Expense - Credit card company management feature></p>

	<ul style="list-style-type: none"> - Required: credit card company ID, password <WORKS Finance - Accounting - National Tax Service Hometax integration> - Required: certificate ID, password <WORKS Attendance - Manage work - Clock-in/out records> - Optional: location information <Implementation inquiries> - Required: name, email address, mobile phone number, company name, business category - Optional: job position <Free setup support service request> - Required: name, email address, mobile phone number, company name
Ncloud Chat	<Service subscription> - Required: admin ID, password
Backup	<Service subscription> - Required: ID, password
Cloud Connect	<Service subscription> - Required: name, mobile phone number, address
Blockchain Service	<Service subscription> - Required: ID, password
Media Connect Center	<Service subscription> - Required: admin ID, password
Video Player Enhancement	<Media Analytics Service subscription> - Required: admin ID, password
Data Teleporter	<Task creation> - Required: name, contacts, address
GAMEPOT	<Service subscription> - Required: admin ID, password
Pinpoint Cloud	<Service subscription and user information entry> - Required: admin ID, password, name - Optional: mobile phone number, email address, department name

④ The Company collects personal information via the following methods:

1. Website, written documents, fax, phone, customer message boards, emails, offline collections (event registrations, seminar attendance)
2. Data provided by partner companies
3. Collection using information collecting tools

Chapter 2 Personal Information Provision and Processing Consignment

Article 4 (Provision of Personal Information to Third Parties)

- ① The Company shall use the Customer's personal information for purposes notified in Article 1 Purpose of Processing Personal Information and shall not exceed this scope without prior consent from the Customer or externally disclose personal information of the Customer as a general rule. However, exceptions are made for cases falling under Articles 17 and 18 of the Personal Information Protection Act, as described below.
1. If the customers have agreed in advance
 2. If required based on the provisions of laws and regulations, or if requested by an investigation agency according to the procedures and the methods set forth in the laws and regulations for investigation purposes.
- ② Provision of personal information after the customer's prior consent occurs in the following cases.

Receiving party	Information Provided	Purpose of use	Period of retention and use
LINE WORKS Corp	Partner member ID, member's name	Japanese partner program's provision and support	For the duration of the partner service
NAVER Cloud Platform partners	Partner member ID, member's name	Partner program's provision and support	For the duration of the partner service
NAVER Cloud Platform partners	Name, email address, mobile phone number	Provision of technical support in relation to the solution	For the duration of the partner service
NAVER Cloud Platform partners	- Required: email address, mobile phone number, company name - Optional: name	Sales inquiry support	Destroyed immediately after fulfillment of purpose
FASTFIVE Didim365	Name, email address, mobile phone number, company name	Provision of free setup support for NAVER WORKS	6 months
TmaxSoft	email address, service usage information	Provision of technical support service for JEUS, WebtoB	Technical support service usage period
TmaxData	email address,	Tibero technical support	Technical support ser

Receiving party	Information Provided	Purpose of use	Period of retention and use
	service usage information	service provided	vice usage period
NVIDIA	email address, service usage information	Technical support for Clara Parabricks	Technical support service usage period
BusinessOn Communication Co., Ltd.	email address, business registration number, business public certificate, (when signing up for SmartBill) business information registered to WORKS Management Support	WORKS Finance Electronic Tax Invoice SmartBill service integration	Service usage period
APPMarket	Admin ID, email address, name	AppMarket service provision	Service usage period
Application operators that have integrated the feature to login with NAVER Cloud Platform account	Member identifier (member ID), name, email address	Provision of member information for application's single sign on login	Service usage period

Due to the frequency of changes in agreements between the Company and its partners, it is difficult for the Privacy Policy to be constantly updated to reflect each new change. For the Customers who utilize the services of NAVER Cloud Platform partners, the list of partners is provided in a website link.

- [NAVER Cloud Platform partner list](#)

- [APPMarket partner list](#)

Article 5 (Consignment of Personal Information Processing)

- ① The Company entrusts the following entities with processing Customers' personal information as needed to deliver or improve services. The Company also enacts provisions to keep personal information secure when entering into agreements with these organizations, in accordance with applicable laws and regulations.
- ② The consigned company entrusted to process the company's personal information and the details of the entrusted work are as follows. If there is a re-entrusted company, it will be disclosed through the link to the consigned company's privacy policy.

Consigned company	Consigned tasks	Period of personal information retention and use
NAVER Corp. (Link)	System operation consignment for service provision, identity verification	Until membership is withdrawn or the consignment agreement is terminated
NAVER FINANCIAL Corp.	Usage fee payment, prevention of payment theft	
NIT Service Corp.	Operation of customer service, security control service, and security service	
N Tech Service Corp.	Service development and operation	
inComms, Greenweb Service Co., Ltd.	service operations	
KCP, Hyosung fms (Link), Toss payments (Link), KSNET	Processing payment (credit card, bank transfer, refund account authentication, cash receipt issuance)	
InfoBank Corp., CJ OliveNetworks Corp. (Link)	Text message delivery system operation	
Hanmac Software Co., Ltd., Simplekey Co., Ltd.,	AI contact center service support	
Nbase Korea Corp.	Game service and chat service support	
SOLIDENG Co., Ltd.	Data transfer related service support	
SimPlatform Co., Ltd.	IoT service support	
Astron Security Co., Ltd.	Integrated cloud security management service support	
JinInfra Co., Ltd.	Network secure communication service support	
SGRSOFT Co., Ltd.	Video Player related service support	
Mixwith Co., Ltd. (Link), Hancm Inc. (Link), PMG Integrated communications Co., Ltd.	Marketing event planning and operation	

Article 6 (Overseas Retention of Personal Information)

- ① The Company does not provide the personal information of users to other businesses overseas. However, for Global Region customers, we process minimal user information in the Global Region country of customer's choice for retention and customer support purposes.
- ② If you do not wish to transfer (store) your personal information overseas, the service cannot be provided. Please withdraw your membership if you do not wish to transfer your information.

Processing grounds for international	Article 28-8 (1) (3) of the Personal Information Protection Act(Consignment/Storage of Processing for Contract Performance)
Person to receive (Person to retain)	NAVER Cloud dl_ncloud_privacy@navercorp.com
Transferred country	Global Region country of customer's choice (Singapore, Japan, Hong Kong, U.S., and Germany)
Transfer date and method	Transferred through a dedicated private network
Transferred personal information items	Minimal membership information required to operate and support Global Region services
Period of retention and use	Consistent with the terms set forth in this Privacy Policy

Only when applying to participate in a survey or event on NAVER Cloud Platform through Typeform, the minimum personal information (name, company name, department, position, contact information, email address) will be transferred (saved) to Typeform in Spain (security@typeform.com) in the form of a network transfer each time the application is completed. Transferred information will be destroyed as soon as the survey closes or event promotion ends.

Chapter 3 Personal Information Destruction Procedures and Methods

Article 7 (Procedures and Methods for Destroying Personal Information)

- ① In principle, the Company will destroy, without delay, the Customer's personal information once the purpose for its collection and use has been satisfied.
- ② If the personal information retention period agreed by the information subject has elapsed or the purpose of processing has been achieved, but it is still necessary to retain the personal information in accordance with internal policies and other related laws (Article 2 Processing and Retention of Personal Information), then the personal information shall be transferred to a separate DB (or a separate document container for paper files) and safely stored for a certain period before being destroyed.
- ③ The following are the procedures and methods for destroying personal information.

1. Discarding procedure

- 가) The Company establishes a personal information destruction plan for personal information that must be destroyed and destroys such information. It selects the personal information for which the reason for destruction has occurred, and destroys the personal information with the approval of the Company's personal information security officer.

2. Destruction methods

- ㄱ) Personal information printed on paper will be destroyed by shredding or incinerating.
- ㄴ) Personal information saved in electronic formats will be deleted via a technical deletion method that destroys data permanently.

Chapter 4 Rights of Customers and Legal Representatives

Article 8 (Rights and Obligations of the Information Subject and Legal Representatives and Method of Exercise)

- ① Customers and their legal representatives may exercise their rights to view, correct, delete, or request suspension of processing of personal information at any time against the Company.
- ② The rights of Customers and their legal representatives can be exercised directly on the "My Page > Manage account" page, or by contacting the Company through "Contact us" or the personal information security officer.
- ③ Customers and their legal representatives can view or edit their registered personal information from "Change member information (My Page > Manage account > Change member information)" at any time after going through the identity verification process. They can request to withdraw from membership (withdrawal of consent) from "Withdraw from membership (My Page > Manage account > Withdraw from membership)."
- ④ Alternatively, the Customer may contact the Company's personal information manager in writing or via phone or email. The Company will process the request without delay.
- ⑤ In the event that a customer has requested to correct personal information, the relevant personal information will not be used until it is updated. In addition, if incorrect personal information has already been provided to a third party, then the third party will be notified about the change without delay.
- ⑥ The Company handles the personal information canceled or deleted by the Customer or the legal representative as specified under Article 2 (Processing and Retention of Personal Information) and ensures that the information can't be viewed or used for any other purposes.

Chapter 5 Technical and Administrative Measures for the Protection of Personal Information

Article 9 (Measures to Ensure Personal Information Safety)

The Company takes the following technical and administrative measures to secure the safety of its Customers' personal information and prevent loss, theft, disclosure, alteration, or distortion thereof.

1. Password encryption

Member passwords are encrypted one-way for storage and management. Only the member knows their password, and only the member who knows their password can access the account to view or modify their personal information.

2. Measures against hacking or other attacks

The Company exerts every effort to prevent any hacking attacks or computer viruses from leaking or damaging the members' personal information. The Company backs up data frequently to prevent personal information loss and uses up-to-date vaccine (anti-virus) programs to prevent leaks or damages to personal information or data. The Company uses encrypted communications to allow safe transmission of personal information on the network. The Company also controls unauthorized access using an intrusion prevention system and exerts every effort to have in place every technical mechanism possible to ensure the security of the system.

3. Minimization of personal information handling employees and their training

Personal information handling is limited to the persons in charge only. For this purpose, a separate password is provided, which is constantly renewed on a regular basis. Compliance with the privacy policy is always emphasized through frequent training of the persons in charge.

4. Operation of the dedicated privacy organization

We are making efforts to make corrections and adjustments immediately if a problem is discovered by checking the fulfillment of privacy policy and compliance of the persons in charge through an in-house privacy task force, etc. However, the Company does not bear responsibility for damages that are not caused by the negligence of the Company, such as the Customer's own negligence or accidents in areas not managed by the Company when the Company has fulfilled the obligations to protect personal information.

Chapter 6 Installation, Operation, and Refusal of Automatic Personal Information Collection Devices

Article 10 (Installation, Operation, and Refusal of Automatic Personal Information Collection Devices)

- ① The Company uses "cookies" that save and frequently retrieve Customer information to provide personalized and customized services.
- ② Cookies are small text files sent to the Customer's browser by the server that hosts the Company website, and they are sometimes stored in the hard disk of the Customer's computer. When the Customer visits the Company website again, the website server reads the content of cookies and uses it to maintain the Preferences of clients and to provide customized services.
- ③ Cookies do not automatically or actively collect information that identifies individuals, and customers can refuse or delete these cookies at any time.

1. Purpose of cookies

- 가) Cookies are used to provide users with optimized and customized information by identifying the type of visit and use of each service and website visited by the user, and whether the user has a secure connection.

2. Installation, operation, and rejection of Cookies

- 가) Customers have the right to choose whether to install cookies or not. Thus, customers can allow the use of all cookies, opt to provide confirmation each time a cookie is saved, or reject the use of cookies entirely by specifying options in the web browser.
- 나) The Company uses log analysis tools, such as Google Analytics and Adjust, for service usage and statistical analysis. If you wish to stop analyzing logs through external analysis tools, then you can cancel the setting through the guide page below.
 - [Guide to turning off Google Analytics settings](#)
 - [Guide to turning off Adjust settings](#)

3. If the Customer rejects cookie usage, the Customer may experience difficulties in accessing some of the Company's services that require login.

Chapter 7 Policy Regarding Location-Based Service

Article 11 (Period of Retention and Use of Personal Location Information)

- ① The Company retains and uses the personal location information for the minimum period required to provide location-based services.

- ② The Company destroys, without delay, the personal location information after using the information one time or temporarily in most of the location-based services. However, if the personal location information is saved along with other content in the service, the information is stored together for the content retention period or user-defined retention period.

Article 12 (Grounds and Period of Retention of Data Confirming the Collection, Use, and Provision of Personal Location Information)

The Company automatically records the data confirming the use and provision of the location information regarding the subject of personal location information based on Article 16, Paragraph 2 of the Act on the Protection, Utilization, etc. of Location Information, and retains it for 6 months or more.

Article 13 (Procedures and Methods of Destruction)

The Company destructs personal location information without delay once the purpose of processing is accomplished in a manner it cannot be recovered or restored.

Article 14 (Provision and Notification of Personal Location Information to Third Parties)

- ① The Company does not provide personal location information to a third party without the consent of the subject of personal location information. If the Company provides a third party provision service, then the Company notifies the subject of personal location information in advance and obtains consent.
- ② If the Company provides personal location information to a third party specified by the subject of personal location information, then the Company immediately notifies the subject of personal location information of the person to receive, time of provision, and purpose of provision every time the communication end device is used to collect personal location information.

Receiving party	Purpose of provision	Information provided
The company of NAVER WORKS members who use Attendance clock-in/out records based on current location	Verification of clock-in/out location	Current location
NAVER WORKS members participating in the chat room where the link of current location is shared	Location sharing	Current location
NAVER WORKS members invited to the schedule where the link of current location is shared	Specifying location for the schedule	Current location

- ③ However, the Company notifies via the communication end device or email address that the subject of personal location information specified in advance.
 1. The relevant communication end device that collected the personal location information does not have the feature for receiving text, audio, or video
 2. The subject of personal location information asked the Company to notify via the communication end device other than the one that collected the personal location information or email address in advance
- ④ In the case of Paragraph 3, if the particular Member does not notify the Company or does not follow the Company's guidelines after notification, the Company is not responsible or liable for any disadvantages that may occur.

Article 15 (Rights and Obligations of the Person Responsible for Protection of Children at the Age of 8 or Younger, etc. and the Methods to Exercise Them)

- ① If the person responsible for the protection of a person falling under the following cases (hereinafter “child at the age of 8 or under, etc.”) agrees to the use or provision of personal location information for the protection of the lives or physical safety of a child at the age of 8 or under, etc., then the Company is deemed to have the consent of the person themselves.
1. Child at the age of 8 or under
 2. Adult ward
 3. Person with a mental disability in accordance with Article 2, Paragraph 2, Subparagraph 2 of the Act On Welfare Of Persons With Disabilities who is deemed to be a person with a severe disability in accordance with Article 2, Subparagraph 2 of the Act On The Employment Promotion And Vocational Rehabilitation Of Persons With Disabilities (It is only applicable for those who registered as a person with disability under Article 32 of Act On Welfare Of Persons With Disabilities.)
- ② The person responsible for the protection of a child at the age of 8 or under, etc., who would like to consent to the use or provision of personal location information for the protection of the life or physical safety of the child must submit written consent with a document proving that they are the person responsible for that child's protection. The person responsible for the protection of the child at the age of 8 or under may exercise the entirety of rights of subjects of personal location information if they consent to the use or provision of personal location information of the child.

Article 16 (Information of Location Information Security Officer)

Location Information Security Officer is a concurrent position with Personal Information Security Officer as laid out in Article 17.

Chapter 8 Other

Article 17 (Contact Information of the Personal Information Security Officer and Personal Information Security Manager)

- ① The Company designates persons in charge of personal information protection as follows to take overall responsibility for the processing of personal information and to handle complaints and damage relief related to the processing of personal information.

Personal Information Security Officer		Personal Information Security Manager	
Name	Hanyong Park	Name	Sujin Lee
Department	Security Policy&Privacy	Department	Security Policy&Privacy
Telephone	1544-5876	Telephone	1544-5876
email	dl_ncloud_privacy@navercorp.com	email	dl_ncloud_privacy@navercorp.com

- ② Customers can report complaints related to personal information protection, which occurred while using the company's services, to the Personal Information Security Officer or the responsible department. The Company will promptly provide an adequate reply on the reported details of customers.

- ③ Customers can make a request for access to personal information under Article 35 of the Personal Information Protection Act to the responsible department. The Company will work to ensure that customers' requests for access to their personal information are processed promptly.

Article 18 (Remedies for Infringement of Rights)

The information subject may apply for dispute resolution or consultation to the Personal Information Dispute Mediation Committee, Korea Internet & Security Agency's Personal Information Infringement Report Center, etc. to receive relief from personal information infringement. Please contact the following agencies to report or consult about other personal information infringements.

The following organizations are separate from the Company, and Customers may contact them if they're not satisfied with the results of the Company's own personal information complaint handling or damage relief, or if they need further assistance.

- Personal Information Dispute Mediation Committee (<https://www.kopico.go.kr>/1833-6972 without area code)
- Personal Information Infringement Report Center (<https://privacy.kisa.or.kr>/118 without area code)
- Cyber Investigation Bureau of the Supreme Public Prosecutor's Office (<http://www.spo.go.kr>/1301 without area code)
- Korean National Police Agency Cyber Investigation Bureau (<https://ecrm.police.go.kr> /182 without area code)

Article 19 (Exceptions)

Please note that this "Privacy Policy" is not applicable to personal information collected by the websites linked to the Company's internet service.

In addition, this "Privacy Policy" applies only to members who have signed a service contract with the Company. It does not apply to information subjects handled through services (NAVER WORKS, WORKBOX, GAMEPOT etc.) operated under the management of members. The personal information processing policy applied to the information subject must be verified through the personal information protection manager of each company (organization).

Article 20 (Obligation to Notify)

If any details are added, deleted, or modified in the privacy policy, then the Company will notify the Customers through "Announcements" of its website at least seven days in advance.

However, the Company will make an announcement at least thirty days in advance if there is an important change in the Customers' rights, and the Company can obtain the Customers' consent again if necessary.

Addendum - For U.S. Customers

The Addendum herein ("Addendum") shall be applied only to people who are located or reside in the U.S. or its territories, or to customers accessing service(s) provided in the U.S. This Addendum is part of the Privacy Policy, which is a prerequisite for the Addendum. In the event of an inconsistency in the Privacy Policy and the Addendum, the terms set forth in the Addendum shall prevail, as long as they are specified in the Addendum. Any term not specifically defined in the Addendum will follow the definition given in the Privacy Policy.

(1) Customer's Consent

The customer's access or use of the service constitutes the customer's consent to the Privacy Policy.

(2) Additional information about cookies and similar tracking technologies

The Company may collect data from cookies, web sockets, and similar technologies to track the Customers' activity patterns within the Company's services and compile statistics about usage and response rates. Customers have the right to choose whether to install cookies or not and can use all cookies, opt to provide confirmation each time a cookie is saved, or reject the use of cookies entirely by specifying options in the web browser. However, if the Customer rejects the cookie usage, the Customer may experience difficulties accessing some of NAVER's services that require login.

(3) Additional uses and disclosures of personal information

The Company may also use and disclose your personal information as it believes to be necessary or appropriate: (a) to comply with applicable law, to respond to requests from public and government authorities, to cooperate with law enforcement, or for other legal reasons; (b) to enforce its terms and conditions; and (c) to protect its rights, privacy, safety or property, and/or that of its affiliates, you, or others. Additionally, the Company may use, disclose, or transfer the Customer's information to a third party in the event of any reorganization, merger, sale, joint venture, assignment, transfer, or other disposition of all or any portion of its business, assets, or stock (including in connection with any bankruptcy or similar proceedings).

Addendum - For Singapore Customers

The Addendum herein ("Addendum") shall only be applied to customers who are located or reside in Singapore or its territories, or to customers accessing service(s) provided in Singapore. This Addendum is part of the Privacy Policy, which is a prerequisite for the Addendum. In the event of an inconsistency in the Privacy Policy and the Addendum, the terms set forth in the Addendum shall prevail, as long as they are specified in the Addendum. Any term not specifically defined in the Addendum will follow the definition given in the Privacy Policy.

(1) Consent from the customer with respect to the collection, use, and disclosure of personal information

The Customer acknowledges and agrees that the Company may collect various types of information (including personal information) about themselves as set out in Chapter 1 Article 3 of the Privacy Policy, for the purposes set out in Chapter 1 Article 1 of the Privacy Policy.

(2) Personal information retention period

The Customer's personal information will cease to be retained by the Company once the purpose of collecting and using the personal information has been accomplished, unless further retention of personal information is required for legal or business purposes.

(3) Transfers of personal information outside of Singapore

The Company may transfer the Customer's personal information to countries and territories outside of Singapore. During this process, the Company will take the appropriate measures to ensure that the personal information of a user continues to receive a standard of protection that is at least comparable to that provided under the Personal Data Protection Act.

Addendum - For Hong Kong Customers

The Addendum herein ("Addendum") shall be applied only to customers who are located or reside in Hong Kong or its territories, or to customers accessing service(s) provided in Hong Kong. This Addendum is part of the Privacy Policy, which is a prerequisite for the Addendum. In the event of an inconsistency in the Privacy Policy and the Addendum, the terms set forth in the Addendum shall prevail, as long as they are specified in

the Addendum. Any term not specifically defined in the Addendum will follow the definition given in the Privacy Policy.

- (1) Purpose for the collection and use of personal information: The Company will utilize the customer's personal information for "New Service Development and Marketing" purposes, as listed in Chapter 1 Article 1, but only if the user has consented to such use. The customer may choose to opt out from this article free of charge at any time.
- (2) The Company may entrust the processing of its customers' personal information to entities such as those listed in Chapter 2 Article 5 and may, as circumstances require, transfer such personal information to region(s) outside of Hong Kong.
- (3) Period of retention and use of personal information: Notwithstanding the retention periods for information retention set out in Chapter 1 Article 2, the Company will only retain the customer's personal information for as long as necessary for the purpose for which the data was collected.

Addendum - For EU Customers

The Addendum herein ("Addendum") shall be applied only to customers who are located or reside in the EU or its territories, or to customers accessing service(s) provided in the EU. This Addendum is part of the Privacy Policy, which is a prerequisite for the Addendum. In the event of an inconsistency in the Privacy Policy and the Addendum, the terms set forth in the Addendum shall prevail, as long as they are specified in the Addendum. Any term not specifically defined in the Addendum will follow the definition given in the Privacy Policy.

(1) Collected directly in Korea

All personal information collected by the Company for the purpose of providing the service is transferred from the collection stage to the data center located in Korea using secure cryptographic communication. This personal information is then stored for the duration specified in the privacy policy. The Company has implemented appropriate technical and administrative security standards, including industry standard safeguards, to protect Customer privacy.

(2) Rights of the data subject

Customers have the right to request all their personal information stored in NAVER Cloud Platform. Customers can access their own personal information and update it or change the default settings by clicking "My Page." Customers also have the rights to request NAVER Cloud Platform to edit, block, complete, delete, or limit access to their personal information, or to transfer the data to another organization. Customers also have the right to request additional information about the processing of their personal information. In addition, customers can execute their rights to raise objection over NAVER Cloud Platform's data processing under certain circumstances and to rescind their consent to data processing. For any support regarding the rights listed above, customers can contact the staff in charge of personal information for inquiries (dl_ncloud_privacy@navercorp.com).

Addendum - For Japanese customers

The Addendum herein ("Addendum") shall only be applied to customers who are located or reside in Japan or its territories, or to customers accessing service(s) provided in Japan. This Addendum is part of the Privacy Policy, which is a prerequisite for the Addendum. In the event of an inconsistency in the Privacy Policy and the Addendum, the terms set forth in the Addendum shall prevail, as long as they are specified in the Addendum. Any term not specifically defined in the Addendum will follow the definition given in the Privacy Policy. In addition, the definition of terms of the Privacy Policy and Addendum are interpreted in accordance with the

definitions prescribed in the relevant Japanese laws due to the relation wherein the company must comply with Japanese law not specified in the "Act on the Protection of Personal Information".

(1) Address and CEO

- Address: 13 - 15th floor, Pangyo Tech1 Tower 1, 131 Bundangnaegok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea

- CEO: Kim, You-won

(2) Procedures for disclosure of personal information, etc.

Please contact the person in charge specified under Article 18 regarding the request for notification of the purpose of use of company-held personal information, the disclosure, correction, addition, deletion, and suspension of company-held personal data, and the disclosure of third-party provision records, etc.

(3) Security management measures

The Company stores membership information of Japanese residents in Japan. The company aims to retain personal data accurate and up-to-date as needed to achieve the purpose of use, while discarding any unnecessary personal data. Additionally, the Company devises necessary and appropriate security management measures during the handling, use, and storage of personal data to prevent the leak, loss, or damage thereof, following the personal information protection guidelines set by the Japan Personal Information Protection Commission.

- For the proper handling of personal data, personal information handling policies and regulations are complied with.

- Regulations and policies on the handling, use, storage, and disposal of personal data, including the handling method, persons in charge and their duties, are established and complied with.

- A person in charge of personal data handling is assigned, and regular maintenance checks and audits of personal data handling and are executed simultaneously. Furthermore, the results are reported to a person in charge who arranges a system in which they evaluate, review, and search for improvements.

- Matters concerning the confidentiality of personal data shall be specified in the employment rules, and the education and training of employees for the familiarity of security management shall be thoroughly conducted.

- Measures shall be taken to prevent the theft or loss in divisions that handle personal data.

- Information systems that handle personal data shall be equipped with an identification function to be protected against unauthorized access or illegal software. In addition, access permissions can be set as needed, access to personal data can be recorded, analyzed, and stored, and regular checks are made to detect any suspicious malicious access.

- When handling personal data overseas, necessary security management measures are taken after identifying personal information protection systems of the country/region in question.

(4) Compliance with laws, regulations, etc.

When handling pseudonymized information, anonymized information, and personal information, the company complies with the obligations prescribed in relevant laws, guidelines, etc.

Supplementary Provision

This Privacy Policy shall take effect from July 30, 2024.

[View previous privacy policy \(July 11, 2024\)](#)

[View previous privacy policy \(June 27, 2024\)](#)

[View previous privacy policy \(June 11, 2024\)](#)

[View previous privacy policy \(May 2, 2024\)](#)

[View previous privacy policy \(March 28, 2024\)](#)

[View previous privacy policy \(February 1, 2024\)](#)

[View previous privacy policy \(November 30, 2023\)](#)

[View previous privacy policy \(September 28, 2023\)](#)

[View previous privacy policy \(August 29, 2023\)](#)

[View previous privacy policy \(June 1, 2023\)](#)