

The translation below is provided for your convenience only. If there is any discrepancy between the translation in English and the original Korean text (including due to the delay in translation), the original Korean text takes precedence.

## NAVER CLOUD PLATFORM - Privacy Policy

NAVER BUSINESS PLATFORM Co., Ltd. (the “Company”) complies with the privacy regulations of applicable laws, including, without limitation, the Law Regarding the Promotion of Information and Communication Network Use and Protection of Information, the Privacy Protection Act, the Protection of Communications Secrets Act, and the Telecommunications Business Act. The Company hereby establishes this privacy policy (this “Privacy Policy”) based on the applicable laws. The Company will reasonable precautions to protect rights of its service users and customers. The Privacy Policy herein shall be applied to services provided by the Company and the details are as follows:

### Chapter 1. Personal Information to be Collected and Collection Methods

#### Article 1 (Personal Information to be Collected)

- ① The Company collects the following personal information that is necessary for creating accounts, providing customer consultation, and allowing customers to access and use various services:
1. For Individual Member Sign-Up
    - Mandatory Information: Email address, password, name, Birthday, mobile phone number, country, address
  2. For Corporate Member Sign-Up
    - Mandatory Information: Email address, password, name of business, country, phone number, address of business  
(For residents in Korea) name of representative, business registration number, copy of business license
  3. For Registering an Automatic Payment
    - Credit card: Date of birth (business registration number for businesses), credit card number, credit card expiration date
    - (For the Korean corporate members) Bank transfer: Bank name, date of birth (business registration number for businesses), account number
- ② The following information is automatically created or collected while using the service or processing applications for service:
- IP Address, cookies, connection log, visit date, service use records, defective use records, payment records
- ③ The following information is collected for users of certain services of the Company. Such information is retained only while using the specific service:

Classification	Collected information
Q&A	- Mandatory : Email address, Mobile Phone Number
Cash receipt application	- Mandatory : Mobile phone number or cash receipt card number
When being added as a notification recipient	- Mandatory: Name, mobile phone number, email address
For two-factor authentication with SSL VPN	- Mandatory: Name, Email address
For WORKPLACE Expense Managing credit card company	- Mandatory: Credit card company's Login ID and Password

Classification	Collected information
For mobile phone authentication	Name, date of birth, gender, duplication information(DI), connection Information (CI), mobile phone number and carrier (in the case of mobile phone authentication), nationality or residential information (Korean/foreigner)

**Article 2 (Personal Information Collection Methods)**

- ① The Company collects personal information via the following methods:
  1. Website, written document, fax, phone, customer message boards, email, collected at events or seminars
  2. Data received from partner organizations
  3. Collection of data via automated tools

**Chapter 2. Purposes for Collecting and Using Personal Information**

**Article 3 (Performance of Service Agreement and Settlement of Fees for Services Provided)**

- ① The Company collects personal information to provide customers with contents and customized services, deliver goods, issue invoices, authenticate user identities, process purchases and fee payments, and to collect fees.

**Article 4 (Member Management)**

- ① The Company collects personal information to verify user identities for using member services or to comply with identity check requirement under applicable laws, to confirm individual identification, to prevent illegal use and unauthorized use, to confirm account registrations, to prevent duplicate registrations, to validate identities of legal representatives, to archive records for dispute resolution, for civil complaint processing, and to provide notices.

**Article 5 (New Service Development and Marketing)**

- ① The Company collects personnel information for purposes of developing new services and customizing services, providing existing services and posting advertising based on user demographics, validating services, providing event and advertising information, and providing opportunities for customer participation, understanding usage patterns, and developing statistics on customer use of services.

**Chapter 3. Providing and Processing Personal Information**

**Article 6 (Providing Personal Information to a Third Party)**

- ① The Company shall use the personal information of users within the scope specified in Chapter 2 above and shall not exceed this scope without prior consent of the user or disclose personal information of the user to any third party. Notwithstanding the foregoing, however, the following shall be exceptions:
  1. If the users have agreed in advance
  2. If based on the provisions of laws and regulations, or if there is request of an investigation agency according to the procedures and the methods set forth in the laws and regulations for investigation purposes.
  3. The cases where personal information is provided after the user gives consent in advance shall be as below:

Receiving party	Information Provided	Purpose of use	Period of retention and usage
Works Mobile Corp	(When applying for a NAVER CLOUD PLATFORM Workplace package (Collabo, Collabo+)) Email address of the person in charge/external email address	To provide LINE WORKS service	For the duration of providing the services. (Shall be retained for the applicable period if it is necessary under the

Receiving party	Information Provided	Purpose of use	Period of retention and usage
NAVER CLOUD PLATFORM Partners	Customer Login ID, Customer name	To Provide Partner Program services	provisions of applicable laws and regulations.)

- For NAVER CLOUD PLATFORM partner users, we offer the partner list to specify each partner's Privacy Policy as the Company and partners sign agreements so often in a random manner leading to difficulty to update Privacy Policy each time. Each partner name will be linked to the partner's web page.

[NAVER CLOUD PLATFORM Partner List](#)

### Article 7 (Outsourcing of Handling Personal Information)

- ① The Company entrusts the following entities with processing customers' personal information as needed to deliver or improve services and enacts provisions to keep personal information secure when entering into agreements with these organizations, in accordance with applicable laws and regulations.

Entrusted Company	Entrusted Work	Personal Information Retention and Period of Use
NAVER Corp., Ltd.	System operation for service provision, Self-identification, Fee transaction	Until membership is withdrawn or the entrusting agreement is terminated
NIT Service Co., Ltd.	Customer service, security control service and security product operation	
N Tech Service Co., Ltd.	Service product development and maintenance	
Allat, KCP, Inicis, LG U+, Hyundai/Lotte/KB/BC/Samsung/Shinhan/KEB/Hana SK/Citi/Nonghyup/Gwangju/Jeonbuk/Jeju/Suhyup credit card companies	Payment processing (credit card, account transfer, refund account verification, cash receipt issuance)	
InfoBank Corp.	Text messaging service system operation	
Play D Corp., AMC Asia	Online marketing	
NAVER BUSINESS PLATFORM ASIA PACIFIC PTE. LTD	Data retention	
NAVER China	Service operation tool development and maintenance	

Entrusted Company	Entrusted Work	Personal Information Retention and Period of Use
YOUNGWOO DIGITAL	VMware on Ncloud Marketing	

② Detailed information on handling of personal information outsourced by overseas affiliates are as follows:

Entrusted Company	NAVER BUSINESS PLATFORM ASIA PACIFIC PTE. LTD	NAVER China
Location of Entrusted Company	Hong Kong (RM 1808, 18/F HARCOURT RD ADMIRALTY HONG KONG)	China(北京市朝阳区广顺北大街 33 号院 1 号楼福码大厦 B 座 10 层 1001 室)
Dates and Method of Entrustment	January 17, 2019 Remote transmission through a private dedicated network	January 17, 2019 Executes tasks by accessing private system
Contact Information of Data Management Administrator	dl_nbp_privacy@navercorp.com	nv_china_privacy@naver.com
Items of Personal Information to be Entrusted	All data including personal information collected and retained on NAVER CLOUD PLATFORM	Membership information of NAVER CLOUD PLATFORM
Entrusted Work	International data backup(retention) for securing protection of user data against disasters, catastrophe, etc.	Operation tool development for service provision, operation and maintenance
Period of Personal Information Retention and Use	Corresponds with the retention period specified in the Privacy Policy	Corresponds with the retention period specified in the Privacy Policy

#### Chapter 4. Period of Personal Information Retention and Use

In principle, the Company deletes or destroys customers' personal information without delay once the purpose for collecting and using the personal information has been satisfied. However, the following information will be retained for a specified period of time due to the following reasons:

#### Article 8 (Reason for Information Retention due to Company Policies)

Retained Information	Reason for Retention	Retention Period
Record of illegal use	Prevention of illegal use	1 year
Inquiry/partnership details (only if customer gives express consent)	Customer consultation processing	6 months

## Article 9 (Reasons for Retaining Information According to Applicable Laws and Regulations)

The Company retains users' information for periods designated in applicable laws and regulations, when information retention is required thereunder, including, without limitation, the Commercial Law and Act on the Consumer Protection in Electronic Commerce. In this case, the Company will use the information for the purposes specified in the relevant acts and regulations. The retention periods for these purposes are as follows:

Retained Information	Cause for Retention	Retention Period
Record on contracts or subscription withdrawals	Act on Consumer Protection in Electronic Commerce, etc.	5 years
Records on payments and goods supply		5 years
Records on complaint or dispute handling		3 years
Records on display or advertisements		6 months
Ledgers and evidential documents about all transactions as defined by the tax law	Framework Act on National Taxes, Corporate Tax Act	5 years
Records on electronic transactions	Electronic Financial Transaction Act	5 years
Login records	Protection of Communications Secrets Act	3 months

## Chapter 5. Personal Information Destruction Procedures and Methods

In principle, the Company deletes or destroys customers' personal information without delay once the purpose for collecting and using the personal information has been satisfied. The following describes the procedures and methods used by the Company to destroy personal information.

### Article 10 (Destruction Procedure)

- ① The information that the user has submitted for account sign-up will be moved to a separate database (or a separate document container for paper files) and destroyed after retention requirements related to information security in accordance with Company policies and applicable laws are fulfilled (refer to the period of retention and use).
- ② The retained personal information will not be used for any purpose other than for retention as required by applicable laws and Company policies, unless otherwise required by law.
- ③ For reference, the personal information of the members who have not used the service for one year is separately stored and managed in accordance with the 'Personal Information Validity Period Policy'.

### Article 11 (Destruction Method)

- ① Personal information printed on paper will be destroyed by shredding or incinerating.
- ② Personal information saved in electronic formats will be deleted via a technical deletion method that destroys data permanently.

## Chapter 6. User and Legal Representative Rights

### Article 12 (Rights and Methods of Exercising those Rights)

- ① Users and their legal representatives can retrieve or modify personal information at any time or request cancellation of membership.

- ② To retrieve or modify personal information, the user must complete the identity verification procedure on the “Member Information Modification” page of the Company’s website (My Page > Manage Member Information > Modify Member Information).  
To cancel membership (withdraw consent), the user must complete the identity verification procedure on the “Member Withdrawal” page of the Company’s website (My Page > Member Withdrawal).
- ③ In the event that a user has requested to correct personal information, the relevant personal information will not be used until it is updated. In addition, if incorrect personal information is already provided to a third party, the change will be notified to the third party without delay.
- ④ The Company will process deletion without delay if a user contacts the Company’s personal information manager via writing, phone, or email.
- ⑤ The Company handles the personal information canceled or deleted by the user or a legal representative as specified under Chapter 4 above to prevent viewing or using information for other purposes.

## **Chapter 7. Installation, Operation, and Refusal of Automatic Personal Information Collection Devices**

### **Article 13 (Definition of Cookie)**

- ① The Company uses digital files called ‘cookie’ to save and retrieve data for the purpose of providing personalized and customized services.
- ② Cookie is a small text file that is sent to the user’s browser by the server that hosts the Company website and stored to the hard disk of the user’s computer. When the user visits the Company website again, the website server reads the contents of the cookie and uses it to provide customized services.
- ③ The cookie does not collect personally identifiable information automatically or actively and the user can reject the use of cookies or delete saved cookies at any time.

### **Article 14 (Purpose of Using Cookies)**

Cookies are used to provide optimized and customized information, including advertising, to the user by collecting data about the user’s usage patterns, web searches, and time spent on various activities.

### **Article 15 (Cookie Installation, Operation, and Rejection)**

- ① Users have the right to choose whether to install cookies or not. Users can allow 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.
- ② However, if the user rejects cookie usage, the user may experience less than optimal performance for services requiring login.
- ③ Follow the steps below to allow or disable cookie installation in Internet Explorer:
  1. Select Tools > Internet Options menu.
  2. Click the Privacy tab.
  3. Change privacy settings.

## **Chapter 8. Technical and Administrative Protection of the Personal Information**

The Company takes the following technical and administrative measures to secure the safety of user’s personal information and prevent loss, theft, disclosure, alteration, or distortion.

### **Article 16 (Encrypting Passwords)**

Member passwords are encrypted for storage and management and only the user knows the password. As a result, only the user who knows the password can access the account to view or modify the personal information.

### **Article 17 (Measures against Hacking or Other Attacks)**

The Company takes reasonable precautions to prevent any leak or damage to user’s personal information due to hacking attacks or computer viruses. The Company backs up data frequently to prevent damage to personal information. The Company uses up-to-date vaccine programs to prevent leakage or damage to personal information

or data. The Company uses encrypted networks to allow safe transmission of personal information on the network. The Company also controls unauthorized access using an intrusion prevention system. The Company takes reasonable precautions operate and maintain all possible technical systems and equipment regularly to run systems securely.

#### **Article 18 (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 given and updated on a regular basis. Compliance with the privacy policy is always emphasized through frequent training of the persons in charge.

#### **Article 19 (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 shall not bear responsibility for damages that are not caused by the negligence of the Company, such as the user's own negligence or accidents in areas not managed by the Company when the Company has fulfilled the obligations to protect personal information.

### **Chapter 9. Other**

#### **Article 20 (Contact Information of the Privacy Manager and Personal Information Manager)**

Users can report complaints related to personal information protection to the Privacy Manager or Personal Information Manager. The Company will promptly provide an adequate reply on the reported details of the users.

Privacy Director		Privacy Manager	
Name	Jaedong Kim	Name	Hanyong Park
Department	IT Security Center	Department	IT Security Center
Telephone	+82 1544-5876	Telephone	+82 1544-5876
Email	dl_nbp_privacy@navercorp.com	Email	dl_nbp_privacy@navercorp.com

If you need to report on other infringements of personal information or if you require consultation, please contact the agencies below.

- Personal Information Infringement Report Center (<http://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)
- Cyber Safety Bureau of the National Policy Agency (<http://www.ctrc.go.kr> / 182 without area code)

#### **Article 21 (Exceptions)**

Please be noted that this privacy policy is not applicable to personal information collected by the website linked to the Company's Internet service.

#### **Article 22 (Obligation to Notify)**

If any details are added, deleted, or corrected in the privacy policy, we will notify users through the "Announcements" menu of the website at least seven days prior to the amendment. However, we will make an announcement at least thirty days in advance if there is an important change in user's rights, such as collection and use of personal information or providing to a third party.

#### **Article 23 (Language)**

All communications and notices made or given pursuant to the Terms shall be in the Korean language. Provided, that, the Company may provide English translation of the communications and notices for convenience purpose only. In case the Company provides an English language translation of the notices and/or the Terms, the Korean text of such notices and/or the Terms will control in case of any conflict. Notwithstanding the foregoing, however, the Customer may communicate or give notice to the Company in either the Korean or English language.

### **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 a service(s) provided in the U.S. This Addendum is part of the Privacy Policy, which is prerequisite for the Addendum. In case that a statement(s) in the Privacy Policy is inconsistent with that of the Addendum, the Addendum shall take precedence over the policy as expressly provided in the Addendum. Term definitions not specifically referred to in the Addendum will be according to the Privacy Policy.

#### **(1) 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.**

In addition to cookies, the Company may collect data from web socket and similar technologies to, among other things, track the actions of users of the Company’s services and compile statistics about usage and response rates. Users can permit a cookie to be placed or not. By setting up cookies from the Internet options, you can allow all cookies, or check whenever a cookie is stored, or block them all. Please be advised that you can face difficulty when using some services which require login, if you block cookies.

#### **(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.

The Company may use, disclose or transfer your 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 be applied only to people who are located or reside in Singapore or its territories, or to customers accessing a service(s) provided in Singapore. This Addendum is part of the Privacy Policy, which is prerequisite for the Addendum. In case that a statement(s) in the Privacy Policy is inconsistent with that of the Addendum, the Addendum shall take precedence over the policy as expressly provided in the Addendum. Term definitions not specifically referred to in the Addendum will be according to the Privacy Policy.

#### **(1) Consent from a user with respect to the collection, use and disclosure of personal information**

A user acknowledges and agrees that the Company may collect various types of information (including personal information) about him/her as set out in Chapter 1 of the Privacy Policy, for the purposes set out in Chapter 2 of the Privacy Policy.

#### **(2) Personal Information Retention Period**



A user's personal information will cease to be retained by the Company once the purpose of collecting and using the personal information is obtained, and if the personal information is no longer necessary for legal or business purposes.

### (3) Transfers of Personal Information Outside of Singapore

The Company may transfer a user's personal information to countries and territories outside of Singapore. In this regard, 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 2012 (No. 26 of 2012).

## **Addendum for Hong Kong Customers**

The Addendum herein ("Addendum") shall be applied only to people who are located or reside in Hong Kong or its territories, or to customers accessing a service(s) provided in Hong Kong. This Addendum is part of the Privacy Policy, which is prerequisite for the Addendum. In case that a statement(s) in the Privacy Policy is inconsistent with that of the Addendum, the Addendum shall take precedence over the policy as expressly provided in the Addendum. Term definitions not specifically referred to in the Addendum will be according to the Privacy Policy.

(2) Purposes for Collecting and Using Personal Information: We will use your personal information for "New Service Development and Marketing" as listed in Chapter 2 Article 5, only if you have consented to such use. You may choose to opt out from such use free of charge at any time.

(4) Outsourcing of Handling Personal Information: We may entrust processing of your personal information to entities in addition to those entities listed in Chapter 3 and may, as circumstances require, involve transferring your personal information overseas out of Hong Kong.

(5) Period of Personal Information Retention and Use: Notwithstanding the retention periods for information retention set out in Chapter 4, we will only retain your personal information for as long as necessary for the purpose the data was collected.

## **Addendum for EU Customers**

The Addendum herein ("Addendum") shall be applied only to people who are located or reside in the EU or its territories, or to customers accessing a service(s) provided in the EU. This Addendum is part of the Privacy Policy, which is prerequisite for the Addendum. In case that a statement(s) in the Privacy Policy is inconsistent with that of the Addendum, the Addendum shall take precedence over the policy as expressly provided in the Addendum. Term definitions not specifically referred to in the Addendum will be according to the Privacy Policy.

### (1) Transfers of Personal Information Outside the EU

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 and stored during the storage period of the privacy policy. There may be a possible risk that the transfer of personal information abroad may cause to the customer. However, the Company has implemented appropriate technical and organizational security standards, including industry standard safeguards, to protect customer privacy. Specifically, the company received CSA STAR, CSAP, ISO/IEC27001, ISO/IEC27017, 27018, SOC2/3, KOREA ISMS, KOREA PIMS certification.

### (2) Your Rights

You are entitled to ask to be provided with all the information stored in NAVER CLOUD PLATFORM. If you click "My Page," you can update the personal information or default setting. You also have rights to request NAVER CLOUD PLATFORM to edit, block, complete, delete or limit to use your information, or to transfer the data to

another organization. You can ask for additional information about processing your personal information. In addition, you can execute rights to raise objection over NAVER CLOUD PLATFORM's data processing under certain circumstances and to rescind the agreement when asked to give consent for your data processing. If you want the authority described above, contact the staff in charge of personal information for inquiry (dl\_nbp\_privacy@navercorp.com).

**Supplementary Provisions**

This Privacy Policy shall take effect from February 28, 2019.