PRIVACY POLICY

Last Updated: May 27th, 2025

APR Corporation(collectively, ”the Company” or "we", "us", or "our") respects the privacy of all visitors and promises to provide the best service. This Privacy Policy (hereinafter referred to as the "Policies") defines our personal information (defined below) and our policies and practices for its processing through our Services (hereinafter referred to as the "Services").

We are committed to protecting your personal information and security, transparently guiding you how to collect and process it, and complying with privacy laws. When we collect or process your personal information, it is important that you clearly understand the purpose and legal basis of that processing, and what your rights are based on relevant data protection laws. For this purpose, please read this policy carefully.

We value your privacy, and we will protect your rights by complying with the relevant laws and regulations. Your personal information only collects the least amount of information we need to maintain our relationship with you, and we have technical and administrative security measures in place to prevent unauthorized access, change, disclosure, or destruction of your personal information.

You are deemed to agree to this Privacy Policy by accessing or using the Services through computers, mobile phones, tablets, consoles, or other physical or electronic devices (hereinafter referred to as the "Device").

We can modify this privacy policy at any time, and the modifications will be announced on the site. Your continued use of the service means consent to this Privacy Policy and its additional notices and policies. Through the use of the Service, you agree to our Terms of Service and are deemed to accept our privacy practices set forth in this Privacy Policy.

This policy applies to ”**MEDICUBE PRO”**(hereinafter referred to as the "Service") among the services provided by the Company.

OUR NOTICE INCLUDES.

1. INFORMATION AND METHODS OF COLLECTING

(1) Personal Information Items to Collect

We collect the following personal information items.

- Information directly provided by the user for the purpose of using the service
- Account information used to log in to the service (e.g. Google, Apple accounts, etc.)
- When accessing services through mobile apps, authentication tokens and technical information issued by third-party platforms (e.g., browser type, operating system, device type, IP address, device identifier, hardware information, etc.)
- Information provided when linking to an SNS account (user ID, number of followers, number of media, and all other information related to the SNS)
- Campaign-related content information (including all information related to content statistics)
- Financial information (bank account details) required for settlement
- Other information we provide to process your request

In addition to the information, you provided yourself, we may also collect user information provided by our services and third-party services. If you participate in a contest or giveaway sponsored by us, you can collect additional information for the giveaway operation in addition to the information mentioned above.

This information may include publicly available contacts, product sizes, preferences, location information, and other provided information.

We do not collect sensitive information—such as race, political opinions, religious or philosophical beliefs, genetic or biometric data, health information, sexual orientation or sex life, criminal history, or crime-related records—nor do we collect information via location-based services.

(2) Collection method

The company collects your information in the following ways:

- Web pages and mobile apps
- a written form, telephone, e-mail, etc.

2. UTILIZATION OF COLLECTED INFORMATION

We utilize the collected personal information for the following purposes. Some of the items will be used with your prior consent.

(1) Service delivery and management

It provides services to users and processes personal information to smoothly perform necessary management functions.

- Membership Management and Identification
  - ✓ It identifies users through membership registration, self-authentication, and account management, and processes the minimum information necessary to provide services.
- Customer Service
  - ✓ Respond to customer inquiries and requests related to purchase and account information and provide troubleshooting and support.
- User-generated Content (UGC)
  - ✓ Upload your generated content (e.g., reviews, comments, photos, etc.) and enhance the user experience through related features.
- fulfillment of a contract
  - ✓ We process the personal information necessary to fulfill the contract signed between us and you.

(2) service improvement

It provides customized services and utilizes personal information to improve service quality. However, identifiable personal information will not be utilized in this case, and data will be anonymized or de-identified if necessary.

- Improve and personalize services
  - ✓ It enhances the user experience and personalizes the service according to your activities to provide a customized experience.
  - ✓ It can be used to improve existing services or to develop new services based on analysis.

(3) Marketing and Communication

Use personal information to effectively carry out promotions and communications related to marketing activities.

- Marketing and Promotion
  - ✓ It conducts marketing activities such as promotions, events, and surveys, and is used for marketing and advertising with your prior consent.

- Communication
    - ✓ We communicate with you about our products, services, events, and other promotional purposes. It provides messages such as newsletters, promotions, and event guidance.

(4) Compliance with security and legal grounds

We process your personal information to comply with security measures and legal requirements.

- Services and Security
    - ✓ Protect your accounts and services by taking fraud prevention, policy violation detection and prevention, and security measures.
- fulfillment of legal obligations
    - ✓ Personal information can be processed according to the provision of legally required information and requests from government agencies.
    - ✓ It is necessary for us (or the legitimate interests of third parties) and processes your personal information for your benefit realization. In this case, we will consider that your rights do not take precedence over these interests.

3. DISCLOSURE OF COLLECTED INFORMATION

We do not disclose personal information to third parties except in the following cases. Some service providers may be outside of your residence.

- When a company discloses information to affiliates, partners, and service providers
    - ✓ If the Company's affiliates, partners, and service providers perform services for the Company (e.g., billing, order execution, product delivery, and dispute resolution).
- Disclosure resulting from the transfer of business
    - ✓ When it comes to substantial enterprise transactions (e.g. website sales, mergers, asset sales)
- user's prior consent
    - ✓ You choose to receive information about a particular company's products and services.
    - ✓ When a user shares personal information with a site or platform of another company, such as social networking services (SNS).
- legal requirements
    - ✓ Where disclosure is required by law.

- ✓ Where an investigative agency requests disclosure in order to detect a crime.

4. AUTOMATED DECISION MAKING AND PROFILING

The company may collect personal information through cookies.

Cookies are very small text files sent to a user's browser by the server operating the company's website and stored on the user's computer hard drive.

These files are used to evaluate, improve, and customize the user experience, allowing the company to provide better services to users.

For details on the types of cookies and their purposes, please refer to the company's cookie policy.

5. THE PROTECTION OF CHILDREN'S PERSONAL INFORMATION

Generally, we do not collect any information from children under the age of 13 or the equivalent minimum age as prescribed by law in their jurisdiction. Our websites, products, and services are in principle available to the general public.

Our website or application has an age restriction function, so it is not available to children, and we do not intentionally collect children's personal information through that function.

6. OBLIGATIONS AND RIGHTS OF USERS

The user or their legal representative may exercise the following rights regarding the collection, use, and sharing of personal information of the Company as their personal information.

- access to personal information
- Correction or deletion of personal information
- suspension of personal information processing
- withdrawal of personal information consent

To exercise the above rights, users can take relevant actions through the "Modify Member

Information Menu" on the company's website or contact the company's privacy representative or agent by phone or email.

After receiving your request, we will take the necessary action as soon as possible.

However, we may deny your request to the extent that it is legally required, or necessary to fulfill a contract or comply with legal obligations. For example, if fulfilling legal obligations or legitimate business interests are involved, we may restrict the exercise of your rights.

7. INFORMATION SECURITY

We take appropriate technical and organizational security measures to protect your personal information. We are committed to preventing unauthorized access, theft, damage and leakage of personal information. However, since data transmission over the Internet cannot guarantee full security, users are also encouraged to take additional measures to protect their personal information. For example, installing anti-virus software, closing a browser after use, and keeping login credentials and passwords secret.

(1) Retention period of personal information

We hold your personal information for the period required to comply with legal obligations, settle disputes, and fulfill contracts while providing services. The criteria for determining the retention period of personal information are as follows and will be securely deleted after the minimum period.

- compliance with legal obligations
    - ✓ Storage in accordance with legal liability periods and relevant regulatory requirements
- fulfillment of a contract
    - ✓ Keep for the required period under contract with you
- Dispute Resolution and Legal Demand
    - ✓ Keep for the required period under contract with you

(2) Security measures

We take a variety of security measures to protect your personal information. Key security measures include:

- Encryption of personal information

- ✓ When transmitting users' personal information, it uses encrypted communication methods to ensure the safety of data.
- ✓ Important information (for example, passwords) is encrypted and stored securely, and protected from illegal access.

- Response to Hacking
  - ✓ Strengthen the security system to prevent leakage or damage of personal information due to external hacking and computer viruses.
  - ✓ Quickly detect and respond to potential threats through regular security checks and monitoring.
- Internal Management and Access Control
  - ✓ Limit the authority to access personal information to essential personnel in the job and thoroughly monitor their activities.
  - ✓ Access to personal information is prohibited to employees who are not related to their duties, and activity records are tracked and managed for those who are granted access.
- Security Training and Raising Awareness
  - ✓ We provide regular personal information protection training to employees to raise security awareness and to respond quickly and appropriately in the event of a security accident.
  - ✓ All employees must be familiar with and comply with security-related policies and procedures.
- Other than that,
  - ✓ Install an access control system to restrict access to servers or important data that store personal information and prevent forgery and alteration of access records.
  - ✓ Establish and implement internal management plans to thoroughly implement regulations on access and processing personal information.

8. COMPANY CONTACT

If you have any questions or concerns about our service and/or privacy policy, please contact us at the information below.

- APR CORPORATION (36F, 27F, 300, Olympic-ro, Songpa-gu, Seoul, Republic of Korea)

Position	Name	E-mail Address
CPO	Jaehoon Jeong	cs123@apr-in.com
DPO	Sungwook Song	privacy@apr-in.com

9. MODIFICATION OF PRIVACY POLICY

We will update this policy to reflect changes in practices and services and take appropriate action to notify you of any significant changes in accordance with. Posting changes to this policy modifies the "Last Update" date at the top of the policy.

10. PERSONAL INFORMATION PROTECTION POLICY SUPPLEMENT

<1> PURPOSE OF LEGITIMATE PROCESSING OF PERSONAL INFORMATION

A company may only process personal information if at least one of the following applies.

- If the user agrees to process his or her personal information,
- Where processing is necessary for the performance of the contract to which the user is a party or to take measures at the request of the user prior to the conclusion of the contract.
    - ✓ Membership management, identification, etc.
    - ✓ Implementation of a contract concerning the provision of services, payment of fees, settlement, etc. required by users
- Where it is necessary to deal with the compliance of legal obligations applied to the company.
    - ✓ Compliance with relevant laws, regulations, legal procedures, and government requests
- Where treatment is required to protect the significant interests of users or other natural persons.
    - ✓ Detection, prevention, and response to fraud, abuse cases, security risks, and technical problems that may harm users or other natural persons.
- Processing necessary for the performance of duties performed for the public interest or for the exercise of public power attributable to the company
- Where it is necessary for the purpose of legitimate interests pursued by the company or a third party (except when it is ignored by the interests of the data subject or by fundamental rights and freedoms that require the protection of personal data).

<2> THIRD-PARTY SITES AND SERVICES

Our website, product, or service may contain links from third parties, and third-party sites may have different privacy policies. Therefore, users should further check the policies of third-party sites associated with the company site.

The information collected by the company from third parties is as follows.

- Meta Platforms, Inc
  - ✓ Purpose of use: Create a new account using your Facebook account
  - ✓ Information collected: Authentication tokens issued by Facebook
- Google LLC
  - ✓ Purpose of use: Create a new account using your Google account
  - ✓ Information Collected: Authentication Tokens Issued by Google
- Apple Inc.
  - ✓ Purpose of use: Create a new account using the user's Apple account
  - ✓ Information Collected: Authentication Tokens Issued by Apple
- Instagram
  - ✓ Purpose of use: Link the user's Instagram account to monitor the content status
  - ✓ Information Collected: User information (user ID, number of followers, number of media), media information (media ID, number of comments, number of likes)
- TikTok
  - ✓ Purpose of use: Link the user's Tik Tok account to monitor the content status
  - ✓ Information Collected: User information (ID information given to TikTok accounts, user URL, profile name, user name), profile-related statistics (number of followers, followings, likes, videos), image information, image-related statistics (number of likes, comments, shares, views)

<3> CALIFORNIA PRIVACY POLICY

California law provides consumers (Californians) with specific rights regarding their personal information. This California Privacy Rights Notice ("California Notice") complements the APR Privacy Policy. This applies only to California consumers and covers personal information collected online and offline.

If you live in California, please refer to the "California Privacy Policy".

<4> ADDITIONAL STATE-SPECIFIC PRIVACY NOTICE

This state-specific Privacy Notice complements the APR Privacy Policy. Only applicable to consumers located in Colorado, Connecticut, Delaware, Florida, Iowa, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Texas, Utah, and Virginia, covering personal information collected online and offline.

- Categories of personal information collected
    - ✓ Membership management, identification, etc.
- Purpose of processing personal information

Purpose of Processing	Personal Information Items Processed
Customer service delivery and request response	- Identification information (e.g., name, email) - Customer account information (e.g. login ID) - Audio/video material (e.g. call history)
Transaction processing and completion	- Identification information (e.g., name, email) - Personal history (e.g. payment history) - Customer Account Information (e.g. Payment ID)
Delivering personalized services	- Characteristic information (interest)
Promotions, giveaways, and surveys	- Identification information (e.g. email) - Location information (e.g. residence)
Shopping Experience and Product/Service Evaluation	- Identification information (e.g. email) - Customer account information (e.g. login ID) - Personal history (e.g. payment history)
Maintaining mutual records with customers	- Identification information (e.g., name, email) - Customer account information (e.g. login ID) - Audio/video material (e.g. call history)
Service Improvement and Product Evaluation	- Online usage information (e.g., page visit history)
fulfillment of legal obligations	- Identification information (e.g. ID, account information) - Customer account information (e.g. login history)

<5> INFORMATION ON PRIVACY POLICY FOR KOREAN CUSTOMERS

To ensure the safe protection of customers' personal information, we comply with relevant laws, such as the Personal Information Protection Act of Korea, and process information according to the following principles.

- Purpose of Collection and Use
    - ✓ Service provision, customer support, compliance with legal obligations, and other related purposes
- Retention and Usage Period
    - ✓ Personal information is destroyed immediately after the purpose of collection is achieved
    - ✓ However, if retention is required for a certain period under applicable laws, it is securely stored separately from other personal information
    - ✓ Retention periods in accordance with legal requirements:
        - Electronic commerce records: 5 years
        - Records on contracts or subscription withdrawals: 5 years
        - Consumer consultation records: 3 years
        - Tax-related evidentiary documents: 5 years
        - Website visit records: 3 months
- Outsourcing and Provision of Personal Information
    - ✓ Personal information processing may be outsourced for efficient service operation, and information may be provided to third parties when required by law
    - ✓ When outsourcing or sharing information, appropriate protective measures are implemented
    - ✓ Current outsourcing status:
        - Amazon Web Services, Inc. (Korea Region) – Cloud Service
- Overseas Transfer
    - ✓ To operate our services, we may use overseas servers or collaborate with international partners, which may result in the transfer of personal information abroad
    - ✓ In such cases, we comply with relevant laws and regulations to ensure secure processing
- Customer Rights

- ✓ Customers can request to view, modify, delete, or stop the processing of their personal information
- ✓ For inquiries, please contact our Customer Center

- Information Protection
  - ✓ Your personal information is safeguarded by appropriate security measures

<6> ADDITIONAL DISCLOSURES FOR INDIVIDUALS IN THE EEA

Customers residing in the European Union (EU) have the following privacy rights under the General Data Protection Regulation (GDPR).

- **The right to access information**
  - ✓ You have the right to request and view your personal information that we have. This right allows you to learn more about the type of data we have, the purpose of processing, the recipient, and more.
- **The right to correct and delete**
  - ✓ You have the right to correct or delete your personal information we have if it is inaccurate or incomplete. You can also request that your personal information be deleted if you decide that it is no longer necessary to process it.
- **Right to limit processing**
  - ✓ You have the right to limit your privacy processing activities under certain conditions. For example, you can exercise this right if your personal information is incorrectly or illegally processed.
- **Data movement rights**
  - ✓ You have the right to transfer your personal information to another service provider. This right applies only if the information you provided is technically available.
- **The right to withdraw consent**
  - ✓ You have the right to withdraw your consent to the processing of your personal information at any time. Consent withdrawal only affects future data processing, and data processed prior to withdrawal will still be valid.
- **The right to complain**
  - ✓ You have the right to complain to our privacy officers or to complain to your country's privacy supervisory authority in the event of a problem with

the handling of your personal information. In EU countries, complaints can be made to their supervisory bodies.

We are committed to protecting your personal information and are obliged to report and respond to incidents promptly in accordance with the European Union General Data Protection Regulations (GDPR) if they are leaked or other security incidents occur. A security incident refers to any accident, including unauthorized access, change, deletion, leakage, or loss of personal information.

- **Reporting procedures and obligations**
  - ✓ In the event of a security incident, we must notify the relevant supervisory authority within **72 hours**. In addition, if an accident can have a significant impact on you, you should also be notified immediately.
  - ✓ In the event of a security incident, we prepare an incident report including the cause of the incident, the affected data items, the likelihood of the incident on the victim, and actions to respond to the incident, and so on, and submit it to the relevant authorities.
  - ✓ Immediately after the accident, we take additional security measures quickly to deal with the accident and prevent similar accidents in the future.

We can transfer your personal information to various countries and regions in the process of providing services. In particular, for European Union (EU) customers, the legal requirements of their countries must be met when transferring data. As a result, your personal information may be transmitted outside the EU, and this transmission is always done with the protection of your rights as a top priority.

- **Data Transfer**
  - ✓ We may transfer your personal information to countries outside the European Union.
  - ✓ In this case, we take appropriate protective measures to comply with data protection laws. If your personal information is transmitted outside the European Union, the transmission will be based on Standard Contractual Clauses or through a mechanism under relevant laws such as the EU-U.S. Privacy Shield Framework.
  - ✓ We put your privacy first, and we manage to ensure that all data transmission is done legally.

- ✓ You have the right to complain to our privacy officers or to complain to your country's privacy supervisory authority in the event of a problem with the handling of your personal information. In EU countries, complaints can be made to their supervisory bodies.

- **Data Processor**
  - ✓ Your personal information may be processed by a designated data processor.
  - ✓ The data processor processes personal information according to our guidelines, and we are responsible for this.
  - ✓ We enter into a written contract with the data processor and ensure compliance with obligations under the GDPR. Contracts with data processors ensure safe processing and protection under privacy laws.