VUNO Inc. Privacy Policy

(Effective Date: December 9, 2024)

VUNO Inc. (hereinafter referred to as the "Company") hereby notifies users that it has established the following Privacy Policy in accordance with the *Personal Information Protection Act* of the Republic of Korea, to protect the personal information and rights of users and to handle user complaints related to personal information in a smooth and timely manner.

Article 1: Purpose of Processing Personal Information

The Company processes personal information for the following purposes:

- **Provision of services on the website**
  - **Submit Inquiries**: To respond to inquiries (including demo requests), handle complaints, and address disputes.
  - **VUNO Academy**: To provide webinar services.
  - **VUNO Mall**: To execute contracts related to service provision, perform billing and payment, manage members, and conduct marketing and advertising activities.
- **Conduct of clinical trials and research**:
  To verify researcher identity, confirm knowledge of relevant laws, and validate whether the researcher possesses appropriate education, training, experience, and qualifications necessary for conducting research; to determine whether to enter into a contract; to execute such contracts, including the payment of consulting or lecture fees; to resolve

related complaints or disputes; to maintain records verifying the legality and performance of contracts; and to manage data regarding counterparties, contract details, and payment records.

- **Sales and marketing activities**:
  To carry out marketing activities targeting healthcare professionals through various online and offline channels such as visits, phone calls, postal mail (including email), text/KakaoTalk messages, webinars, etc.; to promote the Company's products and services, conduct market research, announce and host conferences or events.
- **Transactional activities**:
  To execute and perform contracts (e.g., identifying and verifying contact persons, supplying products/services, and receiving payments); to resolve related disputes or complaints; to manage relevant communications; to manage computerized records of contracts, transactions, deliveries, and payments; to determine renewal or termination of contracts; and to conclude sponsorship agreements with clubs or organizations, pay sponsorship fees, and provide benefits under sponsorship terms.
- **Customer service and safety information management**:
  To respond to product-related inquiries, verify the identity of complainants, investigate facts, communicate investigation results, report and assess product safety or quality complaints, and manage related information.
- **Recruitment**:
  To verify applicant identity, education, and career history; determine and notify hiring results; confirm reapplication intentions for future recruitment; prevent repeated applications from ineligible candidates; and perform employment contract-related tasks.

- **Media relations**:
  To conduct interviews, receive reports regarding the Company's products, and distribute press releases.
- **Legal and administrative compliance**:
  To fulfill statutory and administrative obligations under relevant laws, including the *Medical Service Act*, *Medical Device Act*, and *Bioethics and Safety Act*, such as conducting clinical research, reporting adverse events, submitting required materials, and meeting reporting obligations on consulting and lecture payments under the *Fair Competition Code* for medical device transactions. It also includes tax-related obligations such as filing and paying corporate and value-added taxes and issuing receipts and tax invoices.
- **Processing video information**:
  To ensure facility safety, prevent fires and crimes, secure transparency in logistics operations, and respond to complaints.
- **HATIVCare Application**:
  To perform membership registration, measurement, service application, and consultation activities.

Additionally, the Company processes **pseudonymized medical data** for the purposes of **developing AI software and conducting research**.

Such medical data does **not** include personal identifiers such as names or contact information. The Company uses the data solely for scientific research purposes and does not process pseudonymized data to identify specific individuals.

Furthermore, pursuant to the *Personal Information Protection Act*, the Company may use or provide personal information within the scope reasonably related to the original purpose of collection, taking into account whether the use or provision causes disadvantage to the data subject, whether security measures such as encryption have been implemented, and other

factors.

Specific considerations include:

1. Whether the new use or provision is related to the original purpose of the collection.
2. Whether the additional use or provision was reasonably foreseeable given the context of collection or processing practices.
3. Whether the use or provision unjustly infringes upon the data subject's interests.
4. Whether necessary safety measures such as pseudonymization or encryption have been taken.

The Company will carefully evaluate these factors in determining whether to use or provide personal information for additional purposes in accordance with relevant laws and regulations.

Article 2: Retention and Processing Period of Personal Information

1. The Company retains and uses personal information for the period specified by law or within the retention and use period agreed to by the data subject at the time of collection, until the purpose of processing is achieved. Once the purpose is fulfilled, the information is promptly destroyed.

- Retention periods by purpose:

Purpose	**Retention Period**
Submit Inquiries	3 years from the date of inquiry submission
VUNO Academy	Until membership withdrawal
VUNO Mall	Until membership withdrawal

Purpose	**Retention Period**
Clinical trials and research	3 years from the date of device approval/modification (for medical device clinical trials); otherwise, 3 years from completion of study. For consulting/lecture data: 5 years from completion.
Sales activities	3 years from the date of collection
Transactional activities	Until contract termination
Customer service and safety info	3 years from the date of collection
Recruitment	1 year from the final hiring decision
Media relations	3 years from the date of collection
Legal/administrative obligations	Until completion of legal obligations (e.g., 3 years from adverse event report date)
Video information	180 days from the date of collection
HATIVCare Application	Until membership withdrawal

Pseudonymized medical data used for scientific research shall be retained and utilized until the research is completed.

2. Additionally, the Company retains certain information for the statutory retention period required by applicable laws, such as the *Commercial Act* and the *Protection of Communications Secrets Act*, as follows:

Record Type	**Legal Basis**	**Retention Period**
Important business documents	Commercial Act	10 years
Records on payment and supply of goods or contract withdrawal	Consumer Protection Act in E-commerce	5 years
Records on consumer complaints/dispute resolution	Same as above	3 years
Records on labeling and advertising	Same as above	6 months
Website visit logs	Protection of Communications Secrets Act	3 months
Clinical trial protocols and implementation records	Medical Device Act	3 years
Human subject research records	Bioethics Act	3 years

Article 3: Provision of Personal Information to Third Parties

1. The Company, in principle, processes personal information only within the scope specified in Article 1 and does not provide personal information to third parties without the prior consent of the data subject. Exceptions apply in the following cases:
    - When the data subject has provided prior consent to the disclosure or provision of information to third parties.
    - When such provision is required or permitted by applicable laws or regulations.
2. Status of third-party data sharing:

[Customer (Healthcare Professional) Information]

Recipient	**Purpose**	**Items Provided**	**Retention Period**
Authorized local distributors by product (e.g., FundusAI: Ahn-Gook Pharmaceutical Co., Ltd.; DeepASR: Puzzle AI Inc.; BoneAge: Speed Dental Inc.)	Product inquiries, explanations, and maintenance	Hospital name, customer name, specialty, email, phone number	Until the intended purpose is achieved

[Researcher Information]

Recipient	**Purpose**	**Items Provided**	**Retention Period**
Ministry of Food and Drug Safety (MFDS)	Application for clinical trial approval under Article 10 of the Medical Device Act	Name, affiliation, phone number	Until the intended purpose is achieved

Same as above	Compliance with sponsor obligations under the Medical Device Act	Researcher's qualifications (name of PI, institution, specialty, position, contact, career, education, clinical trial training history, etc.)	Until the retention period specified under Article 24 and Annex 3 of the Enforcement Rule of the Medical Device Act
Ministry of Health and Welfare	Submission of expenditure reports on economic benefits under relevant laws	Name, affiliation	5 years from the date of report preparation (per Article 13-2(1) of the Medical Device Act)
Korea Medical Devices Industry Association (KMDIA)	Verification of quarterly reporting compliance and fee limits under the Fair Competition Code	Lecture/consulting details (date, venue, purpose, name of the speaker, affiliation, fee, topic)	5 years from January 1 following the year of activity
IRBs/Ethics Committees at participating hospitals	Submission, amendment, or reporting of clinical trial plans, adverse	Researcher qualifications and subject health data (age, sex,	Until the legally required retention period

	events, or noncompliance	medical history, vital signs, test results)	
Relevant government agencies (e.g., Small and Medium Business Administration, KOICA, KHIDI, etc.)	Submission of documentation for national R&D projects	Name, affiliation, contact information of project participants	Until project completion
National Tax Service	Tax filing and reporting under tax laws	Name	Until the intended purpose is achieved

[Shareholder Information]

Recipient	**Purpose**	**Items Provided**	**Retention Period**
Financial Supervisory Service, Korea Exchange	Fulfillment of disclosure obligations	Major shareholder's name, ownership ratio, number of shares	Until the legally required retention period

[Adverse Event Information]

Recipient	**Purpose**	**Items Provided**	**Retention Period**

MFDS and foreign regulatory authorities in product-approval countries	Adverse event reporting under relevant laws	Subject initials, sex, date of birth, age, height, weight, and related health information	Until the legally required retention period

Article 4: Outsourcing of Personal Information Processing

1. The Company entrusts personal information processing tasks to third parties for efficient service operations, as follows:

Trustee	**Entrusted Task**
Doodlin Inc.	Operation of the recruitment website and applicant management
Goorm Co., Ltd.	Coding test administration for applicants
KL Partners, Robert Walters Korea, Alfred HR, InnoSearch, Insight HRG, Manpower Korea, HR Group, Kiss Consulting, Finkers Korea, HR Korea, YourSide, Interfit, RediMe, Easypharm, HTA, Mensch Consulting, Success Korea, Ivy Career	Recruitment outsourcing services
GPlab Inc.	Gifticon delivery services
Intuon Co., Ltd.	Booth production, installation, dismantling, storage, and promotional goods logistics

Trustee	Entrusted Task
Inowing Co., Ltd.	Operation of the VUNO Academy website
Kookmin Bank (Securities Agency Division)	Stock registry management, securities issuance, dividend and bond payment agency services
Samsung Securities Co., Ltd.	Electronic voting management services
D2S Co., Ltd., Seoul CRO Co., Ltd., Cynex Co., Ltd., Promedis Co., Ltd., CRS Cube Co., Ltd.	Clinical trial management, database storage, and management
Inet Hosting Inc.	Server management
Amazon Web Services	Data storage
Google Firebase	Service usage tracking and evaluation
NICE Information Service Co., Ltd.	Identity verification
Korea Post, CJ Logistics	Product delivery

2. The Company stipulates in outsourcing contracts all necessary provisions in compliance with Article 25 of the *Personal Information Protection Act*, including prohibitions on personal information processing for purposes other than contract performance, technical and managerial safeguards, restrictions on subcontracting, management/supervision responsibilities, and liability for damages.

3. If any change occurs in the list of trustees or the contents of entrusted work, the Company will promptly disclose such changes through this Privacy Policy.

Article 5: Entrustment of Personal Information Processing

1. For AI medical device services such as BoneAge, Fundus AI, and Chest X-ray, the Company processes patient information entered by service users (hospitals) solely for the purpose of providing such services.
2. Patient data stored in the system is retained and processed during the service provision period (until the user withdraws membership).
3. Details on user data processing for each service are also available in the respective service-specific privacy policies.

Article 6: Rights and Obligations of Data Subjects and Legal Representatives

1. Data subjects may exercise the following rights regarding personal information protection at any time. However, these rights may be limited due to compliance with other relevant laws.
    - Request for access to personal information
    - Request for correction of errors
    - Request for deletion
    - Request for suspension of processing
    - Withdrawal of consent

2. Requests under paragraph 1 may be made by submitting a written request in accordance with Form No. 8 of the Enforcement Rules of the Personal Information Protection Act to the following address via mail, email, or fax. The Company shall respond without delay.
    - Address: 9F, 479 Gangnam-daero, Seocho-gu, Seoul, Republic of Korea
    - Email: privacy@vuno.co
    - Fax: +82-2-515-6647

    (Consent withdrawal may also be carried out in the same manner used for providing consent.)
3. If the data subject requests correction or deletion due to errors in personal information, the Company will not use or provide such information until the correction or deletion is completed.
4. The rights described in paragraph 1 may also be exercised through a legal representative or an authorized agent. In such cases, the power of attorney in the form prescribed by Form No. 11 of the Enforcement Rules of the Personal Information Protection Act must be submitted.
5. The Company shall verify the identity of the individual or the legitimacy of the agent when such rights are exercised.

Article 7: Type of Personal Information Processing

The Company processes the following personal information items:

(Personal information types include Submit Inquiries, VUNO Academy, VUNO Mall, Clinical Research, Sales, HR, etc.)

Article 8: Destruction of Personal Information

The Company shall promptly destroy personal information when the retention period has expired, the processing purpose has been achieved, or the information is no longer necessary. The procedures, deadlines, and methods for destruction are as follows:

1. Destruction Procedures
    - Personal information collected by the Company is transferred to a separate database (DB) or stored separately (in the case of paper documents) after the retention period has expired or the processing purpose has been fulfilled. It is then stored for a certain period in accordance with internal policies or relevant laws before being permanently destroyed.
    - Personal information transferred to a separate DB shall be solely used in compliance with the relevant laws.
2. Destruction Methods
    - Personal information recorded or stored on paper shall be destroyed by shredding or incineration.
    - Personal information stored in electronic forms shall be deleted using technical methods that render the data irrecoverable.

Article 9: Measures to Ensure the Security of Personal Information

In accordance with Article 29 of the *Personal Information Protection Act*, the Company takes the following technical, managerial, and physical measures necessary to ensure the security of personal information.

1. Managerial Measures
    - Establishment and implementation of internal management plans.
    - Regular training for employees on data protection.
2. Technical Measures

- Management of access rights to personal information processing systems.
- Installation of access control systems.
- Encryption of unique identifiers and other sensitive information.
- Installation of security programs to prevent hacking or data loss.

3. Physical Measures
    - Access control for the central server, data storage, and similar facilities.
4. Additional Measures for Pseudonymized Information
    - In addition to the above, the Company implements the following measures for pseudonymized data:
        1. Separation of pseudonymized information from additional information (additional information shall be destroyed when no longer required).
        2. Separation of access rights between pseudonymized and additional information.
    - Maintenance of records, including:
        1. Purpose of processing pseudonymized information,
        2. Categories of pseudonymized data,
        3. Details of pseudonymized data usage,
        4. Recipients of pseudonymized data, and
        5. Other matters deemed necessary by the Personal Information Protection Commission for effective management.

Article 10: Personal Information Protection Officer

1. The Company appoints a Personal Information Protection Officer responsible for overseeing the Company's compliance with privacy obligations, managing user complaints, and providing remedies related to personal information protection, as follows:

- Name: Jong-Hoon Park
- Department/Title: Head, Software Development Division
- Phone / Email: +82-2-515-6646 / privacy@vuno.co

2. Data subjects may contact the Personal Information Protection Officer or the department responsible for all matters related to personal information protection, complaint handling, or remedies while using the Company's services (or conducting business with the Company). The Company will respond and handle such inquiries without delay.

Article 11: Installation, Operation, and Refusal of Automatic Data Collection Devices

1. The Company uses "cookies" to store and retrieve user information to provide personalized and customized services.
   - A cookie is a small text file sent by the Company's web server to the user's browser and stored on the user's computer hard drive.
   - When a user visits the website again, the server reads the stored cookies to maintain user preferences and provide customized services.
2. Data subjects have the right to choose whether to allow cookies.
   - Users may configure their web browsers to allow all cookies, receive notifications when cookies are stored, or refuse all cookies.

- However, refusal to accept cookies may result in limitations in service provision.

3. Cookie Settings (Example for Internet Explorer):
   - Go to the top menu: Tools → Internet Options → Privacy.
   - Adjust cookie acceptance settings as desired.

Article 12: Installation and Operation of Video Surveillance Equipment

The Company installs and operates video surveillance systems (CCTV) as follows:

Item	**Description**
Purpose and Legal Basis	Facility safety, fire prevention, crime prevention and investigation, transparency in logistics operations, and customer complaint handling
Locations and Number of Devices	2nd Basement (8 units, fixed): 1 at entrance (lobby/corridor), 1 at server room entrance, 3 inside server room, 3 inside HATIV warehouse; 8th floor: 1 at entrance; 9th floor: 1 at entrance; 10th floor: 1 at entrance; 11th floor: 1 at entrance
Manager and Authorized Personnel	Data Controller: Head of General Affairs; Authorized Viewers: Head of Business Support Division, Head of IT Security Infrastructure Team, Head of HR Team, Logistics Manager (for warehouse cameras only)
Recording Time / Retention / Storage Location	Continuous 24-hour recording; retention for 180 days; stored in server room

Item	Description
Processing Method	Access, provision, or destruction of footage is logged; recordings are permanently deleted using irreversible methods once the retention period expires (automatic deletion system).
Access Procedure	Requests to view footage must be submitted to the Data Controller.
Response to Viewing Requests	Access may be granted only to the data subject captured in the footage or where necessary to protect the life, body, or property of the data subject. A written request form must be submitted.
Security Measures	Implementation of internal management plans, access controls, secure storage and transmission technologies, access logs and tamper prevention, and locked storage facilities.
Other Provisions	The Company does not install CCTV in areas where it may severely infringe privacy, such as bathrooms, dressing rooms, or saunas, and does not use audio recording or manipulate CCTV arbitrarily.

Article 13: Links to Third-Party Websites or Applications

The Company's website may include links to third-party websites, plug-ins, or applications.
When a user clicks or connects to such links, the third party may collect or use the user's personal information.

The Company does not control these third-party websites, plug-ins, or applications and is not responsible for their personal information processing practices.

Article 14: Amendments to this Privacy Policy

1. This Privacy Policy shall take effect from the effective date stated above.
2. In case of additions, deletions, or modifications required by changes in laws or internal policies, the Company shall notify users through the notice section of its website at least seven (7) days prior to the effective date.
3. Revision History:
    - Jan 1, 2020
    - Mar 10, 2020
    - Nov 9, 2020
    - Aug 25, 2021
    - Jan 4, 2022
    - Jan 4, 2023
    - Mar 7, 2023
    - Jul 20, 2023
    - Dec 28, 2023
    - Feb 12, 2024
    - Dec 9, 2024 (current version)