

# Privacy Policy

GI Innovation Inc. (the "Company") will protect personal information and rights of data subjects and comply with the following privacy policy in order to deal with data subjects' complaints related to personal information, in accordance with applicable laws such as the Personal Information Protection Act.

## Article 1. Purpose of Processing Personal Information and Method of Collection

1. The Company will process personal information for the following purposes. Personal information will not be used for purposes other than the following purposes, and without the relevant data subject's prior consent, personal information will not be used beyond the scope and purpose of use nor be disclosed to a third party.
  - **the Company's pharmaco-medical research activities:** conducting pharmaco-medical research and development activities (such as analyzing data collected from clinical trials), making decisions whether to request for lecture, consulting or research, and record-keeping for notification purposes, etc.
  - **the Company's execution and delivery of contracts:** identifying a party to a contract, making decisions whether to enter into a contract, performing obligations of contracts (such as making payments in consideration for receiving products and services), making contacts for contract purposes, responding to defaults of contracts, dealing with contract-related disputes and complaints, evidencing the execution and delivery of contracts, and managing computerized systems on contract status including contract partners, contents of the contracts, and payment details, etc.
  - **the Company's performing legal or administrative duties:** reporting adverse events in accordance with applicable laws such as the Pharmaceutical Affairs Act, conducting internal audits, conducting tax declaration and payment (such as income tax and value-added tax), performing other legal or administrative duties (such as issuing receipts and tax invoices) levied on the Company by applicable laws, regulatory authorities, administrative agencies, and government agencies, etc.
  - **the Company's conducting marketing and pharmaco-medical information communication activities:** participating in market research, academic seminars, meetings,

training, and other activities for communicating pharmaco-medical information to and from health professionals, handling and responding to questions and complaints, etc.

- **handling recruitment-related administrative affairs and proceeding with recruitment process:** identification of real names and personal certifications, confirmation on willingness to apply during future recruitment drives, replying to questions related to recruitment, retention of documents for the issuance of documents after resignation, and confirmation on willingness to preserve the documents after a mandatory period of preservation, etc.
  - **visitor identification, crime prevention, and facility safety for security purposes**
  - **handling complaints and providing answers to questions regarding the Company, etc.**
2. The Company will collect your personal information in the course of monitoring the Company's tech tools and services including but not limited to emails, phone calls, fax, and other written forms. In addition, the Company will collect or create your information when you provide the Company with your information or communicate directly with the Company.

## **Article 2 Personal Information to be processed**

1. Personal information items to be processed by the Company are as follows:
- Health professionals' name, birth date, health institutions' name and address, title, phone number, cell phone number, fax number, email address, mail address, medical license number, resident registration number (alien registration number), passport number, specialty (education and work experience), bank account number, business registration number, etc.
  - Information collected in the course of conducting clinical trials based on patients' explicit consent and performing obligations under applicable laws related to clinical trials: patients' name (or patient ID, initials or other coded identity information), birth date, gender, health information related to disease (including health professionals (or doctors) who diagnosed and prescribed and the health institutions (or hospitals) they belong to).
  - Information on the Company's contract partners such as suppliers, shipping companies, translators, financial or legal advisers, and other consultants and contractors (if the partner is a corporation, the partner's directors, officers, and employees who are in charge of the transaction with the Company are included): e.g. their name, phone number, cell phone number, fax number, email address, office address, resident registration number, business

registration number, bank account number, work experience and qualifications.

- Job applicants' name, photo, gender, birth date, address, contact number, email address, nationality, education, major, grade or academic achievement, language skills, work experience, military records, cover letter, etc.
- Information to be automatically collected or created in the course of the performance of work or the use of services: data subject's entry and exit records, browser types, OS, access records (IP address, access time), etc.
- Submitters' name, email address, contact information, etc.

### **Article 3 Period for retention and use of personal information**

In principle, the Company will destroy personal information of a data subject without delay when the purpose of its collection and use has been achieved as above, unless such information has to be retained in accordance with applicable laws.

### **Article 4 Provision of personal information to 3rd parties**

1. The Company will process personal information within the scope described in this Privacy Policy, and will not process or provide personal information of a data subject to a 3<sup>rd</sup> party beyond the scope without the data subject's prior consent, except during the following events in accordance with applicable laws:
  - in the event that the data subject's consent to the disclosure and provision is obtained; or
  - in the event that such provision is required or allowed by applicable laws or required by a competent investigative agency in accordance with due methods and procedures for investigation purposes; or
  - in the event that it is deemed manifestly necessary for the protection of life, bodily or property interests of the data subject or third party from imminent danger where the data subject or his or her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses; or
  - in the event that pseudonymized information is provided for statistical purposes, scientific research purposes, and market research purposes.
2. The Company will provide personal information to 3<sup>rd</sup> parties as below.

**<Current Status of the Company's Provision of Personal Information to Third Parties>**

Correct as of: 5th July 2021

<b>Recipient (Contact Information)</b>	<b>Purpose of use by recipient</b>	<b>Personal Data to be provided</b>	<b>Period of use and retention by recipient</b>
National Tax Service (126)	Tax declaration and payment of income tax, etc. Submission of payment statement for earned income, retirement income, etc.	Name, resident registration number of a person who is a party to a contract with the Company. Employees and their family members' year-end tax adjustment information, etc.	Until the date when the purpose of use is achieved
Four Social Insurance entities (National Pension, National Health Insurance, Employment Insurance, Industrial Accident Compensation Insurance)	Management of Social insurance qualification and requirements	Employees and their family members' resident registration number (alien registration number), address, contact information, income, etc.	Until the date when the purpose of use is achieved
Regulatory Authorities (Ministry of Food and Drug Safety in Korea (1577-1255), etc.)	Clinical study protocol review application (amendment submission), adverse drug reaction reporting, final report submission, etc. in accordance with applicable laws	Health professionals(Investigators)' name, title, contact information, health institutions(or hospitals)' name and address, adverse event information, patients(trial subjects)' age, birth date, height, gender, weight, medical history, disease name, drug name,	Until the date when the purpose of use is achieved

		and other health information at the time of occurrence	
--	--	--	--

## Article 5 Outsourcing personal information processing

The Company outsources personal information processing to external professional companies stated below. Any change in the outsourced companies and the outsourced services can be found on the Company's Privacy Policy webpage at <https://www.gi-innovation.com>. Outsourcing the processing of the employees' personal information will be found on the Company's internal bulletin board.

### <Current Status of the Outsourcers>

Correct as of: 5th July 2021

Outsourced company name	Description of outsourced services
Clinical Trial Service Providers in and outside Korea (Syneos Health, LLC, Syneos Health UK Limited, etc.)	All or part of the sponsor's tasks and roles related to clinical trials (e.g. Project Management, Handling and Storage of clinical trial documents, Monitoring, Data Management, etc.)
ADT CAPS (1800-6400)	Unmanned security services & CCTV management

## Article 6 Installation and Operation of Visual Data Processing Devices

The Company will install and operate visual data processing devices as below, pursuant to the Personal Information Protection Act.

### 1. Purpose of installation and operation of visual data processing devices:

- Ensuring the safety and security of facilities
- Crime prevention, e.g. theft

### 2. Location and scope of filming;

Location	Number of devices	Place and scope
Building A (Rooms 1114 to 1117)	Two CCTVs  One Network Video Recorder (NVR)	Passageways, entrances/exits  Document room

Building B (Rooms 1014 to 1017)	Two CCTVs  Two NVRs	Passageways, entrances/exits  Document room
---------------------------------	---------------------------	---

### 3. Management personnel and authorized personnel

The management personnel is in charge of managing the operation of the devices, protecting data subjects' visual data and dealing with complaints related to such visual data. In addition to the management personnel, the authorized personnel is authorized to have access to the data.

	Name	Title	Department
Management personnel	Sung-jin Park	Head of Team	Information Strategy Team
Authorized personnel	Jun-yeong Jeong	Team Member	HR Team

### 4. Duration of filming, retention period, retention place and processing method of the visual information:

Duration of filming	Retention period	Retention place and processing method
24 hours	Building A: up to [60] days from the date of filming  Building B: up to [90] days from the date of filming	Saved in NVR in a document room

### 5. Outsourcing of the installation and management of visual data processing devices:

Outsourced Company Name	Purpose and scope of outsourced services	Contact details
ADT CAPS	Installation, maintenance, and operation of visual data processing devices	1800-6400

### 6. How and where to check the visual information:

A data subject can check his or her visual information in the head office or branch office where the data subject wants to check such information, after submitting an access request to the Company and obtaining the prior approval from management personnel.

#### **7. Measures to deal with the data subject's request to access the visual information:**

A data subject may request to access his or her personal visual information by submitting the request to the Company to access, verify the existence of, or delete such visual information. The Company will allow such access, verification, or deletion:

- only for footage containing the data subject;
- otherwise only when it is necessary for the protection of life, bodily or property interests of the data subject from imminent danger

When visiting the head office or branch office to access such information, the visitor must bring the request form (review, confirmation of existence, deletion), and the following documents to confirm his/her identity as the data subject or the data subject's appointed representative:

- If the visitor is the data subject: proof of identity of the visitor as the data subject
- If the visitor is an appointed representative of the data subject: document proving the appointment of the visitor as a representative of the data subject (e.g. power of attorney), and document proving the identity of the visitor

The data subject's request can be rejected by the Company in any of the following cases:

- When the personal visual information has been destroyed after the retention period
- When there are other legitimate reasons to reject such a request

In the case of rejection, the data subject will be notified of the reasons for rejection in writing or other means within 10 days.

#### **8. Measures for ensuring safety of visual information:**

The personal visual information that the Company processes is managed in a safe and secure manner using encryption measures and the following:

- Establishment and implementation of internal policies for the safe processing of personal visual information
- Measures to control and restrict access to personal visual information

- Application of technology to store and transmit personal visual information securely (e.g. encrypted transmission of network camera feeds and passwords)
- Measures to prevent forgery and modification of stored access logs and records, e.g. creation date/time of personal visual information, purpose of access, identity of visitor, date/time of access etc.
- Physical measures and locking facilities to provide and ensure safe and secure storage of personal visual information.

## **Article 7 Rights of Data Subjects and Exercise of Rights**

1. A data subject may exercise the following rights regarding the collection, use, sharing of personal information by the Company in accordance with applicable laws such as the Personal Information Protection Act:

- the right to access to his or her personal information;
- the right to make corrections or deletion;
- the right to make temporary suspension of treatment of personal information; or
- the right to request the withdrawal of their consent provided before;

at any time by sending Form 1-1 [Personal Information (Access, Correction, Deletion, Processing Suspension, Withdrawal of Consent) Request] or Form 1-2 [Personal Visual Information (Access, Confirmation of Existence, Deletion) Request] by e-mail to the Company or the DPO of the Company.

**<Form 1-1> Personal Information (Access, Correction, Deletion, Processing Suspension, Withdrawal of Consent) Request** [<download link>](#)

**<Form 1-2> Personal Visual Information (Access, Confirmation of Existence, Deletion) Request** [<download link>](#)

2. A data subject can exercise the rights provided in Section 7.1 through an agent, including a legal representative and a power of attorney ("Representatives") by sending Form 2 (the Power of Attorney) by e-mail to the Company or the DPO of the Company.

**<Form 2> the Power of Attorney** [<download link>](#)

3. The Company will take measures regarding the request from data subjects or their Representatives without delay, in accordance with applicable laws such as the Personal Information Protection Act.

However, where any of the following is applicable, the Company may notify the data subject of the reason and deny the request of such data subject:

- Where special provisions in other laws so require or it is inevitable to observe legal obligations;
- Where access may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of any other person;
- Where it is impracticable to perform a contract such as the provision of services as agreed upon with the said data subject without processing the personal information in question, and the data subject has not clearly expressed the desire to terminate the agreement.

#### **Article 8 Destruction of Personal Information**

- The Company will destroy a data subject's personal information immediately after the personal information becomes unnecessary owing to the expiration of the retention period, attainment of the purpose of processing the personal information.
- Despite the expiration of the retention period or attainment of the purpose of processing the personal information, where the Company is obliged to retain the personal information under other laws and regulations, the relevant personal information or personal information files will be transferred to another database or stored and managed separately from other personal information.
- The personal information stored in electronic files will be destroyed using technical means to prevent the recovery of the records, while personal information preserved in paper documents will be shredded or incinerated.

#### **Article 9 Measures for Ensuring Safety of Personal Information**

The Company, in accordance with Article 29 of the Personal Information Protection Act, takes the following technical, administrative and physical measures necessary to ensure safety:

- Establishment and implementation of internal management plan
- Minimizing the number of personnel in charge of handling personal information and conducting education about personal information protection
- Installation of security programs and conducting of regular updates and checks/scans

- Measures to control and restrict access to personal visual information
- Use of encryption and appropriate measures for safe storage and transmission of personal information
- Measures to prevent forgery and modification of stored access logs and records in the case of data breaches
- Physical measures and locking facilities to provide and ensure safe and secure storage of personal information.

## **Article 10 Data Protection Officer**

To protect personal information and deal with complaints related to personal information, the Company designates the following Data Protection Officer (DPO).

### **[Data Protection Officer]**

- Name: Sung-jin Park
- Office and position: GI Innovation Inc., Head of Information Strategy Team
- Tel.: +82 70 7700 3862
- E-mail: niceca@gi-innovation.com
- Address: Building A, #1116, 167 Songpa-daero, Songpa-gu, Seoul, 05855 the Republic of Korea

## **Article 11 Remedies for Violation of Rights and Interests**

A data subject may file a petition for settlement of a dispute, consultation, etc. with the Personal Information Dispute Mediation Committee, the Korea Internet and Security Agency or the Personal Information Infringement Reporting Center to seek remedies for the breach of privacy. In addition, you may contact any of the following agencies to report or receive counselling on the breach of privacy:

- Personal Information Infringement Reporting Center (Korea Internet and Security Agency): 118 (without area code) (<https://privacy.kisa.or.kr>)
- Personal Information Dispute Mediation Committee: 1833-6972 (<https://www.kopico.go.kr>)
- The Cyber Crime Investigation Team of the Supreme Prosecutors' Office: 1301 (without area code) (<https://www.spo.go.kr>)

- The Cyber Terrorism Response Center of the National Police Agency: 182 (without area code) (<https://cyberbureau.police.go.kr>)

## **Article 12 Storage, use, and denial of automatic collection of personal information**

In order to provide users with personalized services, the Company can save and use cookies from time to time.

A cookie is a small piece of information sent from the web server to and stored in the user's computer browser and the user's computer hard disks.

- Purpose of the use of cookies: to optimize the user's experience when browsing the website by storing the user's usage mode, personal search terms, and security settings.
- Storage, use, and denial of cookies: to deny the use of cookies, select Tools > Internet Options -> Privacy to access the settings for cookies.
- Please note that the website and other services may not function properly if you deny the use of cookies.

## **Article 13 Standards on Additional Use and Provision of Personal Information**

In accordance with Article 15 (3) or Article 17 (4) of the Personal Information Protection Act, the Company may use or provide personal information without the consent of the data subject, by considering the following matters:

- Whether it is reasonably related to the original purpose for which the personal information was collected;
- Whether additional use or provision of personal information is foreseeable in light of the circumstances under which the personal information was collected and processing practices;
- Whether additional use or provision of personal information does not unfairly infringe on the interests of the data subject;
- Whether the measures required to ensure security such as pseudonymization or encryption have been taken.

## **Article 14 Amendment of Privacy Policy**

In case of modification of this Privacy Policy in accordance with applicable laws and internal policies, the Company will, without delay, make a public notice of such modification or amendment in such a way as prescribed by applicable laws.

Effective Date: 12th July 2021