GROUNDHOG INC.

PERSONAL DATA PROTECTION MANAGEMENT MEASURES

Last Amendment Date: December 9, 2021

Notice To Readers

This English version is a machine-translated of Chinese version and is not an official document of Groundhog Inc. If there is any discrepancy between the English and Chinese versions, the Chinese version shall prevail.

Article 1

To ensure that the execution of the Company's business complies with the Personal Data Protection Act ("PDPA"), the European Union's General Data Protection Regulation ("GDPR"), and other applicable laws and regulations, and to clarify the personal data protection objectives that employees should follow, the Company collects, processes, and utilizes personal data within a reasonable scope. This establishes the basis for the Company's business operations and internal personnel management regarding the use of customers' and employees' personal data, reduces potential legal risks for the Company and its employees, protects the rights and interests of customers, and safeguards the Company's reputation

Article 2

1. Applicable Parties: This policy applies to all personnel of the Company and its subsidiaries, as well as vendors or consultants who have business dealings with the Company (including their employees or temporary staff).
2. Scope: The protection under this policy covers personal data protected by the Personal Data Protection Act. It establishes regulations regarding the collection, processing, use, and international transfer of personal data to ensure the security of such data.

Article 3

Definitions of Terms:

1. Personal Data: Refers to information relating to a natural person, such as name, date of birth, National Identification Number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical history, medical treatment, genetic data, sexual life, health examinations, criminal records, contact information, financial status, social activities, and any other data that can directly or indirectly identify the individual.
2. Identification by Indirect Means: Refers to data that cannot identify an individual directly, but can identify a specific person only when compared,

combined, or linked with other information.

3. Personal Data File: Refers to a collection of personal data that is established within a system and can be retrieved or organized through automated equipment or other non-automated means.
4. Collection: Refers to obtaining personal data by any means.
5. Processing: Refers to recording, inputting, storing, editing, correcting, copying, retrieving, deleting, outputting, linking, or internally transmitting data for the purpose of establishing or using a personal data file.
6. Deletion: Refers to removing stored personal data from a personal data file so that it no longer exists within the file.
7. Use: Refers to using collected personal data for purposes other than processing.
8. International Transmission: Refers to the cross-border processing or use of personal data.
9. Government Agency: Refers to a central or local authority, or an administrative legal entity, that exercises public powers in accordance with the law.
10. Data Subject: Refers to the individual to whom the personal data pertains.
11. Individual: Refers to a living natural person.

Article 4

The data subject shall have the following rights with respect to his or her personal data, and such rights may not be waived or restricted by special agreement in advance:

1. The right to inquire about or request access to the data.
2. The right to request copies.
3. The right to request supplementation or correction.
4. The right to request the cessation of collection, processing, or use.
5. The right to request deletion.

Article 5

1. When commissioning another party to collect, process, or use personal data, the

Company shall appropriately supervise the commissioned party.

2. The supervision referred to in the preceding paragraph shall include periodically verifying the commissioned party's performance, and keeping records of the verification results.
3. The commissioned party may collect, process, or use personal data only within the scope of the Company's instructions. If the commissioned party believes that the Company's instructions violate the Personal Data Protection Act, the GDPR, or any other personal data protection laws or regulations, it shall immediately notify the Company.

Article 6

The Company shall respect the rights and interests of data subjects when collecting, processing, or using personal data, and shall act in good faith. The scope of such activities shall not exceed what is necessary for the specified purpose, and shall have a legitimate and reasonable connection with the purpose of collection.

Article 7

The Company shall not collect, process, or use personal data relating to an individual's medical records, medical treatment, genetic data, sexual life, health examinations, or criminal records. However, this restriction does not apply under any of the following circumstances:

1. Where explicitly required by law.
2. Where necessary for the fulfillment of a legal obligation, and appropriate security measures are in place.
3. Where the personal data has been made public by the data subject or has been legally disclosed by other means.
4. Where necessary to assist a government agency in performing its statutory duties or necessary for the Company to fulfill its statutory obligations, and appropriate security measures have been taken before or after such use.

5. Where the data subject has provided written consent. However, if the collection, processing, or use exceeds the necessary scope of the specified purpose, or if other laws impose restrictions that cannot be overridden solely by written consent, or if the consent is contrary to the data subject's true intent, the data may still not be collected.

Article 8

The term "written consent" refers to a written expression of intent made solely by the data subject after the Company has clearly informed the individual of the purpose and scope of use, as well as the impact that consenting or not consenting may have on his or her rights and interests.

Article 9

1. When the Company collects personal data from a data subject, it shall clearly inform the data subject of the following matters:
   (1) The name of the Company.
   (2) The purpose of collection.
   (3) The categories of personal data being collected.
   (4) The period, area, recipients, and methods of use of the personal data.
   (5) The rights that the data subject may exercise under Article 4 and the methods for exercising such rights.
   (6) The impact on the data subject's rights and interests if he or she chooses to provide personal data voluntarily but decides not to provide it.
2. The notification required in the preceding paragraph may be exempted under any of the following circumstances:
   (1) Where exemption from notification is permitted by law.
   (2) Where the collection of personal data is necessary for fulfilling a legal obligation.
   (3) Where providing the notification would impede a government agency in performing its statutory duties.

(4) Where providing the notification would impede the public interest.

(5) Where the data subject is already aware of the information that should be provided.

(6) Where the collection of personal data is not for profit and does not have any adverse impact on the data subject.

Article 10

1. If the Company collects personal data not provided directly by the data subject, it shall, before processing or using such data, inform the data subject of the source of the personal data and the matters that must be disclosed.
2. The notification required in the preceding paragraph may be exempted under any of the following circumstances:
   (1) Situations exempted from notification as specified in Paragraph II of the preceding article.
   (2) Where the personal data has been made public by the data subject or has been legally disclosed by other means.
   (3) Where it is not possible to provide notification to the data subject or their legal representative.
   (4) Where it is necessary for statistical or academic research purposes in the public interest, and the data has been processed by the provider or collected in a manner that makes it impossible to identify a specific data subject.

Article 11

The Company shall, upon the request of the data subject, respond to inquiries, provide access, or supply copies of the collected personal data. However, this shall not apply under any of the following circumstances:

1. Where disclosure would endanger national security, diplomatic or military secrets, the overall economic interests, or other significant national interests.
2. Where disclosure would impede a government agency in performing its statutory duties.

3. Where disclosure would harm the significant interests of the Company or a third party.

Article 12

1. The Company shall maintain the accuracy of personal data and shall correct or supplement it proactively or upon the request of the data subject.
2. If the accuracy of personal data is disputed, the Company shall proactively or upon the request of the data subject cease processing or use of the data. This does not apply if processing or use is necessary for the performance of duties or business and the dispute is noted, or if the data subject has provided written consent.
3. When the specific purpose for which personal data was collected no longer exists or the retention period expires, the Company shall proactively or upon the request of the data subject delete, cease processing, or cease using the personal data. This does not apply if processing or use is necessary for the performance of duties or business or if the data subject has provided written consent.
4. If the data subject believes that the personal data has been collected, processed, or used in violation of these regulations, the Company shall proactively or upon the request of the data subject delete, or cease collection, processing, or use of the personal data.
5. For personal data that has not been corrected or supplemented due to reasons attributable to the Company, the Company shall notify any recipients who have previously been provided access once the data has been corrected or supplemented.

Article 13

1. In the event that personal data is stolen, leaked, altered, or otherwise compromised, the Company shall investigate and notify the data subject in an appropriate manner.

2. Upon becoming aware of such a breach, the dedicated unit shall report it to the data protection authority within 72 hours. However, this does not apply if the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the report cannot be made within 72 hours, the reason for the delay shall be clearly stated.

Article 14

1. The data subject may request the Company to respond to inquiries, provide access, or supply copies of his or her personal data. The handling unit shall respond to the request within fifteen days; if necessary, the period may be extended by an additional fifteen days, and the reason for the extension shall be provided to the requester in writing.
2. The Company may charge a reasonable fee to cover necessary costs for responding to inquiries, providing access, or supplying copies of personal data.

Article 15

1. The data subject may request the Company to delete, or to cease the collection, processing, or use of, his or her personal data.
2. The handling unit shall respond to such a request within thirty days, stating the method of handling and the reasons, and obtaining approval from the dedicated unit through a formal report or other appropriate means.
3. All documents and records related to the handling of such requests shall be properly filed and maintained.

Article 16

1. The Company shall collect or process personal data for a specific purpose and under one of the following circumstances:
   (1) Where explicitly required by law.
   (2) Where there is a contractual or similar relationship with the data subject, and appropriate security measures have been adopted.

(3) Where the personal data has been made public by the data subject or has been legally disclosed by other means.
(4) Where the data subject has provided written consent.
(5) Where necessary to promote the public interest.
(6) Where personal data is obtained from generally accessible sources. However, this does not apply if the data subject has significant interests that warrant greater protection against the processing or use of such data.
(7) Where there is no infringement on the rights and interests of the data subject.

2. When the collector or processor becomes aware, or is notified by the data subject, that the processing or use of personal data is prohibited under the proviso of Item 6 in the preceding paragraph, the Company shall proactively or upon the request of the data subject delete, or cease processing or use of, the personal data.

Article 17

The Company shall use personal data only within the scope necessary for the specific purpose for which it was collected. However, use beyond the specific purpose is permitted under any of the following circumstances:

1. Where explicitly required by law.
2. Where necessary to promote the public interest.
3. To prevent risks to the life, body, liberty, or property of the data subject.
4. To prevent significant harm to the rights and interests of others.
5. Where the data subject has provided written consent.
6. Where it is beneficial to the rights and interests of the data subject.

Article 18

The Company shall prohibit the international transfer of personal data under any of the following circumstances:

1. Where it involves significant national interests.
2. Where there are specific provisions in international treaties or agreements.

3. Where the receiving country does not have adequate legal protections for personal data, creating a risk of harm to the rights and interests of the data subject.
4. Where personal data is transferred indirectly to a third country or region in order to circumvent applicable laws and regulations.

Article 19

1. Personnel of each unit of the Company shall cooperate with the competent central authority or the municipal/county governments in conducting inspections related to the security maintenance of data files, data handling methods upon business termination, restrictions on international data transfers, or other regulatory business inspections.
2. Personnel participating in such inspections who become aware of others' data in the course of the inspection shall be subject to a confidentiality obligation.

Article 20

If any unit of the Company receives a request, compulsion, seizure, or copying action from any administrative authority or foreign government entity that it believes is improper, it shall immediately notify the Company's dedicated unit and initiate a declaration of objection or administrative litigation to safeguard the Company's rights and interests.

Article 21

The Company shall implement appropriate security measures to protect personal data files in its possession, in order to prevent theft, alteration, damage, loss, or disclosure of personal data.

Article 22

1. To prevent personal data from being stolen, altered, damaged, lost, or

disclosed, the Company shall adopt appropriate technical and organizational security measures.

2. The measures referred to in the preceding paragraph may include the following, based on the principle of proportionality relative to the intended purpose of personal data protection:
   (1) Assigning management personnel and allocating appropriate resources
   (2) Defining the scope of personal data.
   (3) Implementing risk assessment and management mechanisms for personal data.
   (4) Establishing mechanisms for incident prevention, notification, and response.
   (5) Internal management procedures for the collection, processing, and use of personal data.
   (6) Management of data security and personnel.
   (7) Awareness promotion and training programs.
   (8) Equipment security management.
   (9) Data security audit mechanisms.
   (10) Preservation of usage records, trace data, and evidence.
   (11) Continuous overall improvement of personal data security maintenance.

Article 23

1. The Company shall establish a “Personal Data Protection Management Task Force”, composed of Company executives and designated personnel, with the following responsibilities:
   (1) Proposing the Company’s personal data protection policies.
   (2) Promoting the Company’s personal data management system.
   (3) Assessing and managing risks related to personal data.
   (4) Proposing plans to enhance employees’ awareness of personal data protection and related training programs.
   (5) Evaluating the infrastructure of the Company’s personal data management system.
   (6) Reviewing, deliberating, and assessing the legality and appropriateness of

the Company's data management system.

(7) Planning other matters related to personal data protection and management.

2. To comply with relevant GDPR requirements, the Company may appoint an EU Representative and a Data Protection Officer (DPO).
3. To comply with relevant GDPR requirements, a Data Protection Impact Assessment (DPIA) shall be conducted when necessary.

Article 24

1. Stakeholders who have any questions or suggestions regarding these regulations may submit written materials to the Human Resources unit for discussion.
2. These regulations shall be adjusted and updated in accordance with the personal data file security maintenance plan established by the relevant central competent authority, and announced by the Company. In the event of any conflict with the laws or regulations of the competent authority, the latter shall prevail.

Article 25

1. Employee Basic Information Form and Personal Data Consent Form
2. Data Protection Impact Assessment Form (DPIA)

Article 26

These regulations shall be announced and implemented after approval by the Board of Directors, and the same procedure shall apply to any amendments.