



Data Privacy Policy

1. Preface

1.1 Objectives

In order to ensure effective protection of personal data and to provide remedial measures for data subjects from personal data breach, the G-Able Group has established a personal data privacy policy as a guideline for personal data management appropriately as follows:

- Knowledgeable people within the Group are required to be responsible for information security.
- Provides the best environment, culture and support to personal information for employees.
- All employees have a thorough understanding of their responsibilities and methods of handling personal data.
- Person wishing to submit data access requests must be aware of the procedures and individuals so that they can be handled quickly and accurately.
- A person must ensure that his/her information is carried out in accordance with the data security principles at all times and will not be accessed by unauthorized persons.
- Any transfer or sharing of the Company data with other entities must comply with the requirements.
- Any use of the new system will be assessed as a risk of damage from the collection or disclosure of personal data subject to this policy.

1.2 Scope of enforcement

This policy establishes the scope to apply to all personal data including sensitive personal data that are obtained, processed, stored, modified, disclosed, or deleted by the Group for conducting business in the form of electronic media, document storage systems, and other media, these will include the Group's data as well as personal data owned by third parties that are liable to the Group under contracts conveying data protection provisions.

This Data Privacy Policy applies to all employees of the Group, whether permanent employees, temporary employees, apprentice, contractors, consultants, or third-party users, who may be subject to disciplinary action against those who fail to comply with the policy, including an order to suspend the collection and processing of personal data.

1.3 Definitions

“Data Subject” refers to natural person who is the owner of the personal data, which the Group collects, uses or discloses personal data, including, without limitation, customers, shareholders, business partners, service providers and stakeholders with the Group.

“Personal Data” refers to any information relating to a person which enables the identification of such Person, whether directly or indirectly, but not including the information of deceased Persons.

“Sensitive Data” refers to personal information relating to race, ethnicity, political opinion, belief, religion or philosophy, sexual orientation, criminal record, health information, disability, labor union information, genetic data, biological data, or any other data which may impact the data subject in a similar manner, as stipulated in the Board's announcements.

“Data Controller” refers to person or juristic person having the authority to make decision about the collection, use, or disclosure of personal data.

“Data Processor” refers to person or juristic person undertaking the collection, use or disclosure of personal data in accordance with an order or on behalf of data controller. Thus, this person or juristic person is not a data controller.

2. Methods of Obtaining Personal Data

The Group collects personal data through the following processes:

- 2.1 Services other than those set forth on our website, such as other goods or services that are operated by us or the Group, without expressly being subject to this policy.
- 2.2 Personal data obtained from the Group.
- 2.3 Personal data obtained from third parties such as agents, merchants or the Group that provide data collection services, business partners, partners, etc.
- 2.4 Personal data obtained by visiting the website, such as the name of the Internet service provider and IP Address through internet access, date and time of visit to the website, pages visited while visiting the website, and the address of the website which is directly linked to the website of the Group.
- 2.5 Application usage behavior where a log of your usage will be collected from the group's applications.
- 2.6 Public Records and Non-Public Records that the Group is legally entitled to collect.
- 2.7 Personal data obtained from governmental or regulatory bodies exercising jurisdiction.

3. Purposes for the Collection, Use and Disclosure of Personal Data

The Group has the objectives for the collection, use, or disclosure of personal data as follows:

- 3.1 For improvement of the Group's products and services, and other services or products in the future, as well as to supervise, maintain and operate in connection with the provision of such services.
- 3.2 For the performance of transactions related to the products or services of the Group.
- 3.3 For the management of the relationship between the Group and the data subject.
- 3.4 For confirmation and/or identification of the personal data subject in accessing the services through various channels or contacting the Group.
- 3.5 For communication, notification and/or receiving information from the Group or any changes that occur of the Group.
- 3.6 For the Group's business operations such as data analysis, inspection, product development, service improvement, service usage analysis, etc.

3.7 For any necessary and appropriate action to:

- 3.7.1 Investigate and prevent acts that may violate the law;
- 3.7.2 Respond to requests from governmental or government agencies, including governmental or foreign governments where the personal data subject resides;
- 3.7.3 Enforce our terms of service and policies related to personal data of the Group;
- 3.7.4 Protect the business operations of the Group;
- 3.7.5 Protect the privacy, safety or property rights of the Group, its personnel and data subjects or others; and
- 3.7.6 Remedy, prevent or limit damage that may occur.

3.8 For legal compliance, officer's investigation or regulators or to comply with rules, regulations or obligations required by law or government.

Other purposes not specified above, the data subject will be notified when the Group has a request to collect personal data. In addition, acquisition of your personal data, the Group will collect, use or disclose your personal data under these purposes only subject to the following conditions:

- a case required by law;
- with your consent;
- for your benefit and consent cannot be made at that time;
- it is necessary for the legitimate interests of the Group, person, or juristic person other than the Group;
- it is necessary for the performance of a contract to which the data subject is a party or for the execution of the data subject's request prior to entering into that contract;
- it is for the benefit of life, health or safety; and
- for the purpose of the investigation of the investigating officer or the court's adjudication.

4. The Collection of Personal Data / Format of Data

The Group will collect data obtained directly from the data subject or from the provision of the Group's services or operations through all channels.

- Personal Data means data about a person that can directly or indirectly identify such person but does not include data of a deceased person, such as name, email address/office address, telephone number, ID card number, date of birth, nationality, gender, marital status, Mac address, or Cookie ID, IP Address.
- Browsing behavior data means data which does not identify a natural person such as browser type, domain, visited websites, access time, and address of the website for supporting the customer. The log will be collected from the Group's application.
- System Data means data which is automatically collected when you login into the Group's website. It could be collected by the cookie, web beacons, login file, script, technical data such as IP Address, browser type, domain, visited websites, access time, address of the website, data while being searched or was looked at when the Group's browser was open and the behavior of using the application.

- Address data means the data received via GPS, WiFi, compass, accelerometer, IP Address or the public post.
- Cookies mean data placed on your computer by a web server. Thereafter, cookies will store or remember the user's data until the user closes the browser or deletes or rejects the cookie. However, the use of cookies will make it easier for users to navigate the website.

5. The Personal Data Retention Period

The Group will retain your personal data only for the necessary duration, considering the purpose of collecting and processing, including compliance with the requirements of applicable law in such matters. The Group will store personal data after a certain period of time and in accordance with the applicable legal period, by storing it in an appropriate storage location according to the type of personal data. However, the Group is obliged to keep personal data even after the statute of limitations has expired, for example, in the case of litigation or legal proceedings, etc.

The Group has established security measures that will be used to communicate to those concerned and have confidence in maintaining security as follows:

- Personal data may not be transferred or stored on any mobile device without strict protection regardless of whether the device is owned by the Group, such as the device must be encrypted.
- All personal electronic should be kept safe with passwords and data encryption.
- All personal data copies, along with any electronic copies stored on removable electronic storage media, should be securely stored in lockable boxes, cabinets or drawers.
- All personal data stored electronically is backed up with offsite storage, all backups are encrypted.

The Group will keep your personal data according to the Administrative Safeguard, Technical Safeguard, and Physical Safeguard to maintain appropriate security in the processing of personal data, that means the confidentiality, integrity, and availability are maintained and to prevent personal data breaches. The Group has established policies, regulations and rules for personal data protection, such as security standards of information technology systems and measures to prevent recipients from using or disclosing information beyond the intended purpose or without their authority. In addition, the Group will periodically update such policies, rules and regulations as necessary and appropriate.

In addition, when processing your personal data is required, employees, personnel, agents and recipients of information from the Group are obliged to keep personal data confidential and secure in accordance with the measures established by the Group.

6. Disclosure and Transfer of Personal Data

The Group will disclose personal data to third parties and/or organizations or external entities only in the following cases:

- The related Groups and the Group of the G-Able Group: share your personal data within the Group for marketing purposes;
- Contractors/Counterparties: in the event that the Group employs contractors to perform any act and your personal data is necessary, contractors are required to protect your personal data and not to use that for any purpose other than to support the activities of the Group; and
- Government agencies, governments or other legal entities: in order to comply with the law, order, request, to coordinate with authorities on matters related to compliance with the law.

Transferring and/or ending personal data abroad

In case of transfer and/or send data aboard, the Group will establish the standards for entering into agreements and/or contracts with business entities, organization to which the personal data will be obtained. It has established standards for personal data protection and aligns with relevant laws to ensure that personal data is securely protected, such as:

- In cases where the Group has a necessity to store and/or transfer personal data for storage.
- Cloud processing, the Group will consider organizations with international security standards that store personal data in encrypted form or other means that do not identify the data subject.

To link personal data with other individuals or entities, the group will display the name of the collector or person who has the right to data. In addition, the Group will provide a record of the data linkage as evidence.

7. Measures to maintain the security and confidentiality of personal data

To ensure that the data subject is confident in managing the risk of personal data that may be unauthorized access, leakage, alteration, loss. The Group therefore realizes the importance of information security as well as complying with internationally recognized standards for information security and business continuity management in accordance with the law.

The Group has measures to protect the privacy of data subjects by limiting access rights to those who need to use such personal data in order to offer products and services and for the service of the Group. Persons authorized to access personal data must strictly adhere to the Group's personal data protection measures and maintain the confidentiality of such personal data. The Group has Administrative Safeguard, Technical Safeguard, Physical Safeguard in accordance with applicable regulatory standards to protect personal data. Any act other than or unauthorized, including the transmission of personal or sensitive information to an unauthorized person or any use that damages the Group, will also be considered a violation of this Policy.

8. Your Rights as a Data Subject

The data subject can exercise the rights in relation to your personal data according to the channels and methods of contact by the Company according to the rights you have as follows:

- Right to access and obtain a copy of your personal data, under the Group's responsibility, as well as request the disclosure of the acquisition of your personal data without your consent.
- Right to obtain personal data relating to him/her from the Group, including the right to request the Group to transmit or transfer such personal data to another data controller when possible by automated means or directly to another data controller, unless by the technical condition it is not possible
- Right to object to the collection, use, or disclosure of personal data.
- Right to erasure, destroy, or to anonymize the data subject
- Right to restrict the use of personal data.
- Right to request for the correction of the personal data.
- Right to withdraw consent, in which you can exercise the right of the data subject to withdraw the consent at any time.

9. Communication

This policy applies to internal communications to all employees, worker, and apprentice in the form of notices/memorandum, and appropriately stored via the website on the intranet for external communication; general person, customer, business partner, alliance which published on the Group's website.

10. Contact Channels

Any questions regarding this data privacy policy can be inquired through the channels specified below:

G-Able Public Company Limited
127/30 Panjathani Tower, 25th Floor, Nonsi Road,
Chong Nonsi, Yannawa, Bangkok 10120
Tel. 02-781-9333

Email: contactcenter@g-able.com
or Data Protection Officer (DPO)
Email: dpo@g-able.com

First Logic Company Limited
127/22, Nonsi Road,
Chong Nonsi, Yannawa, Bangkok 10120
Tel. 02-781-9104
Email: contactcenter@firstlogic.co.th
or Data Protection Officer (DPO)
Email: dpo@firstlogic.co.th

Mverge Company Limited
127/22, Nonsi Road,
Chong Nonsi, Yannawa, Bangkok 10120
Tel. 02-781-9103
Email: contactcenter@g-able.com
or Data Protection Officer (DPO)
Email: dpo@g-able.com

The Communication Solution Company Limited
127/20, Nonsi Road,
Chong Nonsi, Yannawa, Bangkok 10120
Tel. 02-781-9200
Email: contactcenter@g-able.com
or Data Protection Officer (DPO)
Email: dpo@g-able.com

InsightEra Company Limited.
110/1 Krung Thon Buri Road,
BanglampooLang, Klongsan, Bangkok 10600
Tel. 02-781-9102
Email: contactcenter@g-able.com
or Data Protection Officer (DPO)
Email: dpo@g-able.com

Blendata Company Limited.
110/1 Krung Thon Buri Road,
BanglampooLang, Klongsan, Bangkok 10600
Tel. 02-781-9101
Email: contactcenter@g-able.com
or Data Protection Officer (DPO)
Email: dpo@g-able.com

Cybergenics Company Limited.
127/22, Panjathani Tower, 17th Floor, Nonsi Road,
Chong Nonsi, Yannawa, Bangkok 10120
Tel. 02-781-9105
Email : contactcenter@cybergenics.co
or Data Protection Officer (DPO)
Email: dpo@cybergenics.co

11. Monitoring, Review and Update Policy

This policy requires regular monitoring and performance indicators of operational processes in accordance with this policy and reviewed at least once a year, or if there are changes related to business operations, operational process, technological changes, or reports a personal data security breach that may be relevant to this policy.