Privacy Policy

Grundfos (Thailand) Company Limited (hereinafter referred to as the “Company” “we” or “us”) values your privacy and strives to protect the personal data of our customers, clients, personnel, business partners or traders, job applicants and other related parties. This right of privacy is a fundamental right of a person (Privacy Right) that is required to be protected complying with the law and the regulations established, whether you visit us via website, application, or request for services from us. In order to process, collect, or disclose of your personal data, we will set up system to control and supervise it strictly and transparently subject to the standards stipulated by the governing government agencies who is a regulator.

The purpose of this Privacy Policy is to inform the data subject about our practices of your personal data, such as collection, use, disclosure, including but not limited to rights. of the data subject, etc. In addition, this policy is regarded as part of the terms and conditions of our services through our website, our application, or direct services to you in each time. This policy therefore applies to all operational activities related to personal data as the following details:

1. Definition

In this policy,

“Company” means Grundfos (Thailand) Company Limited;

“Person” means a natural person;

“ Personal Data” means any information relating to a Person, which enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased Persons in particular;

“Sensitive Data” means any person data may leading to unfair discrimination, in this policy wherein means, racial, religious beliefs, sexual behavior, criminal records, health data, disability, genetic data, biometric data, or of any data classified by law;

“Incompetent Person” means a person who is a minor, an incompetent person or a quasi incompetent person subject to the Thai Civil and Commercial Code;

“Data Protection Officer” means a person appointed by the Company to work as a data protection officer under the Personal Protection Act B.E. 2562;

“Data Subject” means a natural person who is a personnel, staff, employee, job applicant or any related person, customer, service user, website visitor, visitor of the Company’s mobile application, including executive of the Company and any person who has a legal relation with the Company, hereinafter referred to as a “Data Subject”;

“Website” means a website of the Company which belongs to the Company or service provider, as a case may be;

“Application” means any applications provided by the Company, in addition to the applications that have been changed, updated, updated or supplemented thereafter;

“Data Controller” means the Company having the power or duties to make decision regarding the personal data, obtaining from Data Subject or service provider of Data Subject or performance of contractual obligation with Data Subject, whether directly or indirectly.

“Data Processor” means a person or juristic person who operates n relation to the collection, use, or disclosure of the Personal Data pursuant to the orders given by or on behalf of a Data Controller, whereby such Person or juristic person is not the Data Controller;

“Collection” means an acquisition of personal data;

“Data Processing” means any actions which act on the personal data, whether by automated method or not, such as collecting, recording, organizing, storage, use, disclosing, changing or any other actions causing an availability, compilation, or destruction of personal data.

2. Objectives

This policy is provided to protect personal data of the Data Subject, who transacts, uses a service, has an interest with the Company under following objectives:

2.1 To define the roles and duties of organizations, executives, personnel involved in the personal data.

2.2 To determine procedures, security measures or other measures to protect the personal data pursuant to the law.

2.3 To establish a performance guideline of personnel related to the data processing or other operations in relation to the personal data.

2.4 To build a confidence in the security of personal data to persons, customers, partners, service users, as well as other persons who have an interest or involved in the personal data.

3. General Provisions

3.1 The protection of personal data subject to this policy covers the personal data of clients, medical personnel, nursing personnel, medical support personnel, employees, and other related persons, business partners, contractors, job applicants, students, internships or professional experience, etc.

3.2 We may require a Personal Data Protection Officer (DPO) to review this Privacy Policy at least once a year or where it is necessary for changing to the performance of this Policy. Any changes will be announced by the Company via our appropriate communication channel.

3.3 We will collect, use, or disclose of personal data when we have obtained the consent or explicit consent from the data subject prior to or at the time of such collection, use, or disclosure, or after the time of such collection, use, or disclosure in some cases where it is permitted to do so by the law, unless the Company has made such personal data unidentified or on the ground of legal basis as required by the law as follows:

3.3.1 It is necessary for the performance of a contract.

3.3.2 It is necessary for compliance with a law.

3.3.3 it is necessary for legitimate interests where such interests are overridden by the fundamental rights of the data subject of his or her personal data.

3.3.4 It is necessary for the performance of a task carried out in the public interest.

3.3.5 It is for preventing or suppressing a danger.

3.3.6 It is for the achievement of the purpose relating to the preparation of the historical documents or the archives for public interest.

3.4 A request for consent or explicit consent for collection, use, or disclosure of personal data from the data subject, we shall follow the following principles:

3.4.1 A request for consent shall be explicitly made in a written statement, or via electronics means, unless it cannot be done by its nature. For other means for obtaining of consent, it must be made by convincing evidence showing that the data subject has given his or her consent himself or herself.

3.4.2 In requesting consent from the data subject, the Company shall inform the purpose of the collection, use, or disclosure of the Personal Data. Such request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an easily accessible and intelligible form and statements, using clear and plain language, and does not deceptive or misleading to the data subject in respect to such purpose.

3.4.3 In the event that the data subject is a minor who is not sui juris by marriage or has no capacity as a sui juris person, the request for the consent from such data subject shall be required from the holder of parental responsibility over the child.

3.4.4 In the event that the data subject is incompetent, the consent must be obtained from the custodian who has the power to act on behalf of the incompetent person or in the event that the data subject is quasi-incompetent, the consent must be obtained from the curator who has the power to act on behalf of the quasi-incompetent person.

3.4.5 In case that the data subject or the authorized person according clause 3.4.3 and 3.4.4 would like to withdraw his or her consent given to the Company, the same manner of consent as provided herein shall apply mutatis mutandis to the withdrawal of consent of the data subject. In the event that the withdrawal of consent will affect the data subject in any manner, the Company shall inform the data subject of such consequences of consent's withdrawal.

3.5 We shall collect, use, or disclose Personal Data according to the purpose notified to the data subject prior to or at the time of such collection. The collection, use, or disclosure of

Personal Data shall not be conducted in a manner that is different from the purpose previously notified to the data subject, unless the data subject has been informed of such new purpose, and the consent is obtained prior to the time of collection, use, or disclosure.

3.6 We shall collect the personal data where is necessary for carrying out according to the legitimate purposes and such purposes has been informed to the data subject by the law.

3.7 We will erase or destroy the personal data or make the personal data become the anymous data which cannot identify the data subject after the expiration of period for retention or it is unnecessary for the purpose of collecting personal data or as pursuant to the request of the data subject or the data subject withdraw his or her consent, unless there is a legal ground or government regulation for continuing to keep that personal data.

3.8 We shall maintain personal data safely and consider your privacy and confidential of it as a first priority.

3. The Collection of Personal Data Policy

4.1 The collection, use or disclosure of personal data shall be consistent with the principle of personal data protection as required by the law, that are

(1) the personal data shall collected, used or disclosed with lawfulness, fairness and transparency

(2) the personal data shall collected, used or disclosed subject to the objectives specified by the Company and the Company shall not use or disclose the personal data under limited purposes where is provided therein

(3) the personal data shall collected, used or disclosed sufficiently, relevantly and as necessary for the purposes of such collected, used and disclosed (Data Minimization)

(4) the personal data shall collected, used or disclosed accurately and up-to-date, as it is necessary (Accuracy)

(5) the personal data shall collected, used or disclosed as it is necessary (Storage Limitation) and,

(6) the personal data shall collected, used or disclosed under appropriate security measures (Integrity and Confidentiality), nonetheless, the collection, use or disclosure of personal data shall be carried out pursuant to the purposes and only where is necessary under the limited purposes, or for the direct benefits related to the purposes of collection, which will be notified to the Data Subject prior to or at the time of collection of personal data.

4.2 We collect your personal data where is necessary, whether through our website, mobile phone application for online transactions, such as newsletter, subscription, or requesting for a special assistance from us. This will include offline transactions such as providing services at our office. We may also receive your personal data from services in a request form or from the process of submitting a request for the exercise of rights, questionnaire, or correspondence via e-mail or via SMS, etc. Besides, we may obtain your personal data from third parties such as your family members, relative or closed person, including but not limited to dealers or our service providers, or in some cases may be obtained from government agencies in the event that you have given consent to disclose your personal data or the disclosure of personal data as required by law.

4.3 We will retain personal data for as long as necessary pursuant to the purposes of data processing and the applicable laws. After the retention period or the Company has no right to retain or unable to claim the legal ground for processing the personal data of the data subject, the Company will destroy that personal data by appropriate and consistent with the law.

4.4 In the event that the data subject provides the personal data of related persons, such as spouse, family members or friends, etc. to the Company, for example, it may be specified as an emergency contact. The data subject represents and warrants that the data subject has obtained the consent for the collection, use and disclosure of such personal data in accordance with this Privacy Notice.

4.5 We may store the personal data in Cloud Computing by hiring third party services, whether located in Thailand or in a foreign country, that we have entered into a contract with such

party based on the carefulness and consideration for the security of personal data being processing by the Cloud's service providers.

5. Policy for Use and Disclosure of Personal Data

5.1 Use or disclosure of personal data for purposes where is necessary for benefits that are directly related to the purpose of collection. In the event that the person or organization to whom we may disclose or share your personal data to a data processors, who is necessary for our operations, we require such data processors to maintain your personal data confidentiality and to protect your personal data in accordance with the standards as required by the Personal Data Protection Law, in addition to use your personal data pursuant to the purposes that we have determined or according to the order for such data processors to proceed. The data processors will not be able to use your personal data other than those purposes.

5.2 We are strictly concerned with the right to access by the our employees or they can your personal data as necessary only for the performance of their work and according to the rights stipulated by the Company. In case of necessity to perform tasks that require the right to access of personal data other than their authorization, that employee must seek for the approval from the authorized person at all events.

5.3 The Company's employees shall use the personal data for the purposes of collecting or subject to the consent given by the data subject only, unless there is a legal ground supporting.

5.4 Job admin and the owner of the work system must allow the employees of the Company accessing the personal data only for those employees who is granted and has been approved by an authorized person.

5.5 We may disclose your personal data to any government agency, person or juristic person in order to comply with the law or a court order.

6. Policy for Security of Personal Data

We will protect and collect your personal data appropriately, whether your personal data is provided in a document, file or in an electronic system. This will includ various tools that the Company uses for maintaining the security of your personal data in accordance with the law for the benefit of confidentiality, completeness and availability of personal data, in order to prevent of loss, unauthorized access, use, alteration, modification or disclosure of personal data or any action without legal authority, whereby the Company has established and implemented measures to maintain the security of personal data according to the following guidelines:

6.1 Providing authentication measures, determining the authorization, and accounting in accessing, using, disclosing, and processing personal data in accordance with the Company's information security measures strictly.

6.2 In the event that we send or transfer personal data to a foreign country including the use of personal data to store on any database, in which the service provider or data storage service is in abroad, there must be measures, that are adequate or equivalent to the measures set forth in this policy, protecting personal data, unless it is required by law or required a consent of the data subject. We may also do so after we have informed you the purposes of such action and have obtained your consent. Apart from it, we will inform you of the personal data protection standards that may not be sufficient in the destination country. Personally, we may transfer your personal data oversea withour your consent for the performance of a contract to which you are a party or for the use in processing of your request before entering into that contract or in compliance with the requirements of the Personal Data Protection Act B.E. 2562

6.3 In the event of a breach of our security measures and causing personal data breach or personal data leakage to the public, the Company will notify the data subject as soon as possible as well as informing a remedial plan for damages arising out of any breach or leakage of personal data to the public and such breach or leakage affect the rights and freedoms of the data subject. We shall not be responsible for any damage arising from the use or disclosure of personal data to third parties, including from the neglect or omission to log out from the system by the data subject’s action or any other person who obtained the consent of the data subject.

6.4 We set forth regulations for all personnel complying with when they are required to access the personal data of customers, partners, client, and personnel. The personnel who accesses to those personal data will be the only personnel required and for the purpose of performing their duties only, such as personnel in human resources sections, personnel who supervise and manage the contract between the Company and partners, etc. Such access to personal data of third parties can be done only by the order or as stipulated by the company or the law. In addition, third parties are obliged to maintain confidentiality and protect personal data in accompany with providing technology measures to prevent unauthorized access to a computer.

6.5 We constantly review and evaluate the effectiveness of computer systems in order to maintain the security of personal data in accordance with the measures as required.

6.6 We audit an inspection system to manage the destruction of personal data that is not necessary for the Company's operations.

6.7 In case of sensitive personal data, we will take measures to maintain the security of documents and electronic data in the term of access, control of usage, a system of use and a backup system, an emergency plan as well as a regular risk assessment of the system.

7. Roles and Responsibilities

The Company requires personnel or agencies related to personal data to pay attention and be responsible for collecting, using, or disclosing personal data pursuant to the Company's personal data protection policies and practices strictly by assigning the following persons or agencies, to supervise and examine that the Company's activities correctly and legally subject to the policies and laws on personal data protection.

7.1 Executives at all levels shall be responsible for:

7.1.1 Providing rules and regulations to collect the personal data appropriately for each company in accordance with the policies, practices, laws and international standards.

7.1.2 Arranging a responsible person, such as, agencies or personnel who is responsible to oversee the operations in accordance with the regulations.

7.1.3 In the event that the Company employs a natural person or juristic person in order to carry out the processing of the data, a standardized data protection system shall be provided for screening.

7.1.4 Supervising the implementation of policies, guidelines and regulations, as well as developing and improving such implementation to be more efficient and also ensuring that there is a performance report provided pursing to such policies, guidelines and procedures.

7.2 Section or person designated as a collector, user or discloser of personal data shall be responsible for:

7.2.1 Operating and controlling the processing of personal data, including notification, requesting for a consent, collecting, using, or disclosing of personal data in accordance with the regulations of personal data protection and as required by the law.

7.2.2 Implementing and controlling the appropriate security measures, to prevent loss, access, use, alteration, or disclosure of personal data without authorization or misuse of personal data as set forth in the regulations of Personal Data Protection, including notifying the data controller to aware of the incidents of personal data breaches.

7.2.3 Operating and controlling the deletion or destruction of personal data after the retention period has expired, or that is not related to or beyond the necessity for the purposes collected or as requested by the data subject.

7.2.4 Checking and controlling the personal data to be accurate and up-to-date.

7.2.5 Immediate notifying the PDPA working group or DPO when there is any violation of personal data.

7.6.6 Controlling data records and reporting to relevant person who is responsible for it.

7.6.7 Assessing the risk concerning the personal data which is under theirs responsibility, managing and implementing a measure for reducing risk.

7.3 Data Protection Officer shall be responsible for**:**

7.3.1 Providing advice in various fields relating to the protection of personal data for executives, employees, and business partners of the Company.

7.3.2 Supervising and monitoring the operations of data controller and data processor.

7.3.3 Coordinating and cooperating with the Office of the Personal Data Protection Commission; supposing that, there is a problem concerning the collection, use or disclosure of personal data of the Company, its customers, its partners, or any other related person.

8. The Rights of Data Subject

In some cases, we may request you to identify yourself before exercising your rights as a data subject. In this regard, for your privacy and security, you can exercise your rights under the laws on Personal Data Protection and its exceptions as follows:

8.1 Right to access

The data subject can submit a request for personal data accessing or a request to clarify the acquisition of personal data, that the data subject has not given a consent. The Company will prepare or make a copy of the personal data and related information throughout our communication channels. But all these, the company is entitled to refuse such a request, where is required by the law, court order or the access of such personal data may cause damage to the right and freedom of others.

8.2 Right to rectification

The data subject can submit a request to rectify the personal data to be accurate and up-to-date and not misleading, where the evidence or relevant documents must be presented. If the company considers that such request is non-reasonable, the company will reject the request and record the reason of such refusal as an evidence.

8.3 Right to deletion, destruction, or de-identification

The data subject can submit a request for deletion, destruction, or de-identification of the data subject to the company and the request will be proceeded under the following conditions:

- Where is not necessary to retain the personal data according to the purposes provided.
- The withdrawal of consent is made by a data subject and the company has no legal authority to collect, use or disclose personal data.
- The data subject objects to the collection, use or disclosure of personal data for the performance of public tasks and legitimate interests, and it cannot be objected by the company.
- Personal information is collected, used, or disclosed unlawfully.

However, the company is entitled to reject the request of data subject as follows:

- Retention for the necessity of freedom of expression.
- Retention for the purpose of historical documentation, archives, etc.
- Retention for carrying out the tasks for public interest of the company or complying with state powers that the company is appointed.
- Retention of necessary information to perform legal obligation with the purpose of preventive medicine, occupational medicine, a benefit of public health and others as stated by law.
- For establishment of legal claims, compliance or exercise of legal claims, raising the defense of legal claims or compliance with the law.

8.4 Right to withdraw consent

In the event consent given to the company by data subject, the data subject may submit a request for withdrawal that consent. The Company will proceed pursuing to that request and it shall not affect to any other actions taken prior to the exercising of the right to withdraw. Nevertheless, the company has the right to refuse continuing such request; provided that, there is a restriction on the right to withdraw by law or contract providing a benefit to the data subject.

8.5 Right to data portability

The data subject can submit a request to obtain or transfer his/her personal data to another data controller in an electronic format that can be read or used from automatic device, including the right to verify the transferring of such personal data under the following conditions:

- Must be the personal data obtained a consent by the data subject for collection, use, or disclosure of personal data.
- Collecting, using, or disclosing of personal data for the purpose of providing a service or pursuing to the contract between the data subject and the company.

In addition, the company will refuse to data portability if it is necessary for public interests, legal obligations, breaches of the rights or liberties of others, or it technically cannot be operated by the company. The reason of such refusing will be recorded as evidence thereafter.

8.6 Right to restriction

The data subject can submit a request to restrict the company from using of personal data subject to the following conditions:

- The company is in the process If it can be verified that such data is accurate and complete, the Company can reject the request.
- When the personal data is unlawfully collected, used, or disclosed and the data subject does not exercise his/her right to delete, destroy or de-identified, the data subject otherwise request to suspend that use. The company may reject such request if it can provide others legal evidence for the collection, use or disclosure of personal data.
- Where there is not necessary to retain that personal data, the data subject yet asks to retain it for the establishment of legal rights, compliance with, exercising or raising a legal claim.
- The company is in the process of proving the right to reject of the data subject's request subject to the rights.

8.7 Right to object

The data subject can submit a request to object to the collection, use or disclosure of personal data subject to the following conditions:

- For the performance of public task and for the legitimate interest, the Company will reject any objection if it is proved that there are more important legitimate grounds or for the establishment, compliance with, exercising or raising a legal claim.

- For the purpose of scientific and history research. The company will reject any objection if it is necessary to carry out the tasks for the public interests of the company.

However, the company will record the reason of such refusing as an evidence. If the refusal of objection is not met an exception, the company will not continue to collect, use, or disclose that personal data. It is explicitly separated from other information when the data subject has notified the objection to the Company.

8.8 Right to be informed

The data subject has the right to be informed of the information in the event that the company has received an information directly from the data subject or obtained it from a third party throughout the company's communication channels.

8.9 Right to lodge a complaint

The data subject has the right to lodge a complaint in the event that a data controller, data processor, employee or service provider for data processor violates or fails to comply with the Personal Data Protection Act B.E. 2562.

In addition, the company reserves the right to reject the request in the following cases:

- It is permitted by the law to carry out;

- Personal data is anonymized or is unidentified the data subject;

- The requester does not provide an evidence identifying that he/she a data subject or is authorized to submit such request;

- Such request is unreasonable, for example, in the event that the requester does not have authority or does not submit his/her personal data to the company, etc;

- Such request is a redundant request, for example, a request of the same request/content repeatedly without justifiable reason;

- The Company may determine an expense/ a fee for the processing of request in accordance with the rules prescribed by the Company.

In addition, the Company may need to request certain information from you in order to verify your identity and ensure your right to access personal information. (or to exercise any other rights) in order to comply with security measures that will ensure that your personal information will not be disclosed to persons who do not have the right to access such information

The Company may request some certain information from you to verify your identity and ensure your right to access personal data (or to exercise any other rights) to observe the security measures ensuring that your personal data will not be disclosed to any person, who is not entitled to access such information

The Company will endeavor responding to all legitimate requests within 30 days. In some cases, the Company may take more than 30 days if your request is complicated, or you are submitting more than a request.

9. Improvement, Review or Amendment the Data Protection Policy

The Company may update, review, or amend this policy, whether in whole or in part or from time to time, to be consistent with the law, rules and regulations of authorized authorities, and the Company's operations; provided that, this policy is amended.

10. Hiring of Data Processing Policy

The Company has established guidelines for entering a contract for personal data processing with a third party or juristic person, who is a personal data processor, as follows:

10.1 Prior to hiring a data processor, the Company must assess the service provider systems and personal data protection practices. Supposing that the service provider has no security system or such system is inadequate to entering into a contract, the data processor shall

require the service provider to comply with the regulations or announcements specified by the Company.

10.2 The purpose of employment contract must be specified objectives, retention method, notification of the data subject, using, transmitting, transferring of data, and disposing or erasing the data.

10.3 The parties must sign a Data Processing Agreement (DPA) in accordance with the law or as specified by the Company's regulations.

10.4 Upon the hiring of data processor, the Company shall control its processing following the objective of hiring and control its operation in accordance with the relevant guidelines.

10.5 When the data retention period expires, the Company shall monitor and control the service provider to process that personal data, as well as to delete, destroy, or de-identify data (Anonymized Data) in accordance with the rules and regulations prescribed by the Company or agreed upon.

11. Personal Responsibility Policy

11.1 The Company recognizes the importance of training, provided to educate, and raise awareness concerning the compliance of personal data protection, to executive and all personnel. It is also an obligation of all supervisors to assign personnel related to the personal data in their sections to attend the training strictly, in connection with assessment and follow-up to ensure that such personnel will be able to perform their duties completely and accurately as required by the laws on personal data protection.

11.2 The Company appoints a person or agency who is related to the personal data. Such person or agency must pay attention to the importance and responsibility of collection, use or disclosure of personal data in accordance with this Privacy Policy strictly. Any intention or negligent ordering or performing their duties are considered as a violation of this policy and our personal data protection practices; provided, and/or any damage occurred, such person shall be punished pursuant to the Company’s rules and regulations, in addition to be subject to legal

penalties stipulated for such offense. Nevertheless, if such offense causes damage to the Company and/or any other person, the Company may consider proceeding further legal action.

12. Policy on the use of Personal Data for Marketing Purposes

In addition to the purposes that have been notified to the data subject and pursuant to the provisions of the laws on personal data protection, we will use personal data for marketing purposes, such as sending promotion by post, e-mail and by any other means or direct marketing in order to increase the benefits for a data subject as our clients through products suggestions and any related services.

You can choose for non-receiving of our marketing information from us, unless for the communication as a data subject and/or services that the Company is necessary providing to you, such as issuing a receipt, issuing a medical certificate or any documents supporting medical services, etc.

13. Enforcement of Privacy Policy

This policy is applied to all personal data collected, used and/disclosed by the Company, which is entitled by the Data Subject to the Company to collect and use such personal data (if any), in accompany with any personal data, that is currently collected and will be further collected in the future, in order to use or disclose to other persons pursuing to the scope and objectives stated herein.

14. Contact of Appropriate Authority

If you wish to report a complaint or if you feel that the company not responding to your concerns in a satisfactory manner You can contact and/or make a complaint to the Office of the Personal Data Protection Commission as detailed below;

Office of the Personal Data Protection Commission – PDPC

Office of National Digital Economy and Society Commission

Telephone Number : 0-2142-1033

e-Mail : pdpc@mdes.go.th

15. Contact Us

If there is reasonable reason to doubt or believe that there is any violation of personal data, complaint, or the exercise of Data Subject rights under this policy or the Personal Data Protection Act B.E. 2562, you can contact the company by:

Head of Working Group on Personal Data Protection Act

92 Chaloem Phrakiat Rama 9 Road, Dokmai Subdistrict

Prawet District, Bangkok 10250, Thailand

Telephone Number : (+66) 2 725 8999

Fax Number : (+66) 2 725 8998

e-Mail Address : vphraepriungam@grundfos.com