MITSUBISHI ELECTRIC
Changes for the Better

MITSUBISHI ELECTRIC AUTOMATION (THAILAND) CO., LTD.
Bang-Chan Industrial Estate No. 111 Soi Serithai 54 T. Kannayao, A. Kannayao, Bangkok 10230 Thailand.
Tel: (66) 2517-1326, (66) 2919-9873 Fax : (66) 2517-1328 URL : www.meath-co.com E-mail : support_meath@meath.co.th
บริษัท มิตซูบิชิ อีเล็คทริค ออโตเมชั่น (ประเทศไทย) จำกัด
นิคมอุตสาหกรรมบางชัน เลขที่ 111 ซอยเสรีไทย 54 แขวงคันนายาว เขตคันนายาว กรุงเทพฯ 10230
โทรศัพท์ : (66) 2517-1326, (66) 2919-9873 โทรสาร : (66) 2517-1328 URL : www.meath-co.com E-mail : support_meath@meath.co.th

Privacy Policy

Mitsubishi Electric Automation (Thailand) Co., Ltd. values and respects the privacy of the people we deal with and other information about data subject. This Privacy Policy describes how we collect, use and disclose your personal information along with your right as a data subject. Mitsubishi Electric Automation (Thailand) Co., Ltd. is committed to protect your privacy and complying with the Personal Data Protection Act B.E. 2019 as follows:

Chapter 1 General Provisions

Article 1 (Definition of terms)

The definitions of terms used for this rule are as follows

a) "Company" means Mitsubishi Electric Automation (Thailand) Co., Ltd.
b) "Privacy Policy" means this Personal Data Protection Policy.
c) "Act" means the Personal Data Protection Act B.E. 2019
d) "Personal data" means all kinds of data that can identify an individual.
e) "Sensitive personal data" means personal data that can cause discrimination, bias, or serious disadvantages to individuals. Processing of sensitive personal data requires special attention and is usually restricted or prohibited by laws and regulations.
f) "Data subject" means the individual who is identified or identifiable by reference to personal data.
g) "Processing" of personal data means any operation performed on personal data such as collection, recording, storage, utilization, adaptation, alteration, alignment, combination, disclosure or erasure etc.
h) "Supervisory authority" means an independent public authority which is established by each country or area to supervise the compliance with laws and regulations on personal data protection.
i) "Group Data Protection Officer" means a person appointed by the President of MELCO within the Group who has the overall responsibility and authority on personal data

protection across the Group. The Group Data Protection Officer conducts discussion and promotion of the measures to protect personal data, educate the employees, monitor the implementation and operations and review the effectiveness of the measures.

j) "Person in charge of Information Security" means a person appointed by the President of Group Company within each company who promotes the protection of personal data and communicates with the supervisory authority if necessary.

k) "Data Protection Officer (DPO)" means a person appointed at a group company who has the responsibility and authority on personal data protection in accordance with specific applicable laws and regulations.

l) "Representative" means a person or organization in certain countries and areas where our company has no establishment, who is designated by our company to represent itself.

m) "Employees and other relevant personnel" means all of those who are bound by any contract agreement or employment agreement with our company, including directors, executive officers, executive directors, executive fellows, advisory directors, and advisors as well as regular employees and other loaned or temporary employees from outside companies.

n) "Legal basis" means the foundation for processing of personal data that is considered lawful in designated laws and regulations.

o) "Legitimate interest" means the lawful, specific and realistic interest pursued by our company or by a third party, except where such interest is overridden by the interests or fundamental rights and freedoms of data subjects. For instance, processing of personal data for such purposes as direct marketing, fraud prevention, network or cybersecurity, etc. are based on legitimate interest.

p) "Vital interest" means the interest related to data subject's or a third person's life.

q) "Automated decision-making" means the process of making a decision that has impact on data subjects by automated means such as computers. This includes conducting profiling such as analyzing or predicting job performance, financial conditions, health conditions, personal preferences, interests, reliability, activities, locations, movements, etc. in order to evaluate an individual.

r) "Data Protection Impact Assessment" means an assessment of the impact on personal data protection and discussion of necessary measures performed when a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of individuals.

s) "Personal data asset" means the information asset such as files or documents that contain the personal data, regardless of the quantity of data included or the media (paper, electronic file, etc.) of the asset.

t) "Transfer" means all kinds of operations that make personal data available, including making personal data accessible via a network.

u) "International transfer" means all kinds of operations that make personal data available to individuals or organizations located in a foreign country or area.

v) "Joint control" means two or more companies jointly determining the purposes and means of processing. Processing of personal data conducted by multiple departments within our company should not be considered as "joint control".

w) "External organization" means a natural or legal person, or group other than our company. This includes other companies in the Group.

x) "Right to data portability" means the right of data subjects to receive the personal data concerning them, which they have provided to the company, in a structured, commonly used and machine-readable format and to transmit those data to an external organization without hindrance from the company.

Article 2 (Purpose)

This rule aims to ensure that our company will collect, use and disclose personal data as necessary for the operation under the company's objectives. Personal information is properly handled to protect the rights and interests of individuals and achieve social responsibility in relation to the Company's business activities taking into account the benefits of personal data.

Article 3 (Scope of application)

The scope of application of this rule is as follows:

Target business activities: All our business activities involving processing of personal data

Target divisions : All our divisions including Corporate Office, branch offices, research laboratories, and business sites

Target persons : All of those who are bound by any contract agreement or employment agreement with our company, including directors, executive officers, executive directors, executive fellows, advisory directors, and advisors as well as regular employees and other loaned or temporary employees from outside companies

Target information : All personal data used for our business

Article 4 (Compliance with laws and regulations)

Our company shall comply with the applicable laws and regulations on personal data protection (hereinafter referred to as "applicable laws and regulations"), documents issued by supervisory authorities, etc.

Chapter 2 Framework and responsibility

Article 5 (Assignment of Person in charge of Information Security)

Our company assigns a Person in charge of personal data protection, appointed by the Company's directors, to play a role in promoting the protection of personal data in the company, and plan appropriate measures in accordance with the personal data protection requirements set under the advice of the Managing Director. A framework to ensure appropriate protection of personal data is established in line with the size and business operations of the Company.

Article 6 (Assignment of Data Protection Officer (DPO))

Our company assigns a Data Protection Officer.

Article 7 (Assignment of Representative)

Our company assigns a representative when required by applicable laws and regulations.

Chapter 3 Planning

Article 8 (Principles of personal data processing)

Our company complies with the following principles from (a) to (h) when processing personal data. Our company shall be able to demonstrate its compliance with these principles.

(a) Our company shall process personal data lawfully. (Principle of lawfulness)

(b) Our company shall process personal data fairly and in a transparent manner in relation to the data subject. (Principle of fairness and transparency)

(c) Our company shall collect personal data for specified, explicit and legitimate purposes and not further process the data in a manner that is incompatible with the purposes. When personal data is collected from a third person other than the data subject, our company shall pay special attention to process the data only within the initial purpose. (Principle of purpose limitation)

(d) Our company shall only process personal data that are adequate, relevant and limited to what is necessary in relation to the purpose. (Principle of data minimization)

(e) Our company shall keep personal data accurate and up to date where necessary. Reasonable steps shall be taken to ensure personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. (Principle of accuracy)

(f) Our company shall determine the storage period for which personal data are necessary for the purpose. When the storage period ends or when the data subject requests to erase the personal data, our company shall promptly and securely dispose of, erase, or process the personal data in such a way that individuals cannot be identified. (Principle of storage limitation)

(g) Our company shall take appropriate technical or organizational measures to protect personal data from breaches including unauthorized access, accidental loss, destruction, alteration, or leakage. (Principle of integrity and confidentiality)

(h) Our company shall consider taking protective measures necessary to comply with the principles stipulated in Article 8 at the planning stage prior to conducting the processing of personal data for the provision of products or services or internal management. When our company provides functions protecting personal data that can be set up by data subjects, these functions shall be activated by default. (Principle of privacy by design and default)

Article 9 (Identification of personal data)

Our company shall establish and maintain procedures for identifying all personal data used for our business.

Article 10 (Laws and guidelines and other codes stipulated by the state)

Our company shall establish and maintain procedures for specifying and referring to the laws and guidelines and other codes stipulated by the state related to processing of personal data.

Article 11 (Risk recognition, risk Analysis, and countermeasures against risk)

Our company shall, at each stage of processing of identified personal data, establish and maintain procedures for recognizing and analyzing risks (including leakage, loss, or damage of personal data, violation of relevant laws and guidelines and other codes stipulated by the state, expected financial loss and abasement of social trust, and possible impact on data subjects) and taking necessary countermeasures against those risks.

Article 12 (Documentation and development of policies and rules)

Our company shall establish and maintain policies, plans, rules, etc. that are necessary that are necessary to comply with this rule.

(a) Action plans

(b) Monitoring plans

(c) Education plans

Article 13 (Preparation for personal data incidents)

Our company shall establish and maintain procedures involving the following actions for specifying and addressing personal data incidents such as leakage, loss, and damage of personal data, and violation of this rule by employees.

(a) In accordance with applicable laws and regulations, notifying the data subject concerned of details of leakage, loss, or damage of his/her personal data or making such details easily known to him/her.

(b) Publicly announcing the facts, causes, and measures to the greatest possible extent without delay from the viewpoint of prevention of secondary damages and avoidance of similar incidents.

(c) In accordance with applicable laws and regulations, reporting the facts, causes, and measures to the supervisory authority.

Chapter 4 Implementation and Operation

Section 1 Operational Procedures

Article 14 (Operational procedures)

Our company shall clarify the following operational procedures to ensure the implementation of the personal data protection framework.

(a) Identification of new personal data processing

(b) Check of legal basis and risk for new processing

(c) Identification of processing of high risk

(d) Data protection impact assessment

(e) Notification

(f) Consent

(g) Records of processing activities

(h) Transfer and proper management of personal data (subcontractor management, disclosure to external organizations, joint control of personal data, international transfer)

(i) Education

(j) Response to data subject rights

(k) Document and record management

Section 2 Risk Assessment of Processing

Article 15 (Identification of new personal data processing)

Our company shall check whether the processing is a "new processing" upon initiating a processing of personal data, such as by checking whether any processing in the past has been conducted for the same purpose.

Article 16 (Check prior to new processing)

(1) Our company shall check the following items before initiating a new personal data processing.

(a) Reason for collection

(b) Purpose of the processing

(c) Categories of personal data

(d) Method of collection

(e) Notification to data subjects

(f) Confirmation of consent

(g) Existence of subcontracting, provision, and joint control of personal data

(h) Country / Area where the data subjects reside

(i) Categories of data subjects

(j) Number of data subjects

(k) Legal basis of the processing

(l) Existence of international transfer of personal data

(m) Period of personal data processing

(n) Period of personal data storage

(o) Storage place of personal data

(p) Privacy protection functions of the systems engaged in the processing of personal data

(q) Response to data subject rights

(r) Existence of processing of high risk

(2) With regard to (1)(c), our company shall not process sensitive personal data in principle.

(3) With regard to (1)(k), our company shall consider the imbalanced power between the company and the employees when processing the personal data of employees and shall avoid such processing based on data subjects' "consent" where possible.

Article 17 (Identification of processing of high risk)

Our company shall identify the "processing of high risk" among new processing, which satisfies at least two of the following criteria.

(a) Processing of personal data for evaluation or scoring

(b) Processing of personal data for automated decision-making with legal or similar significant effect

(c) Processing as a systematic monitoring

(d) Processing containing sensitive personal data

(e) Processing of personal data on a large scale

(f) Processing containing a matching or combining of datasets collected for different purposes

(g) Processing of personal data of vulnerable data subjects

(h) Processing of Personal data by innovative use or applying new technological solutions

(i) Processing of personal data which prevents data subjects from exercising a right, using a service or concluding a contract

Article 18 (Data protection impact assessment)

When certain processing of personal data is determined as of high risk through a risk assessment, our company shall consider implementation of data protection impact assessments (DPIA) taking into account the nature, scale and purposes of the processing.

Section 3 Personal Data Collection

Article 19 (Notification)

(1) When personal data is directly collected from data subjects, our company shall notify the following information to data subjects prior to the processing.

(a) Company name, contact details of the company and Data Protection Officer

(b) Purposes of the processing and legal basis of the processing

(c) When the legal basis in (b) is "legitimate interests", the contents

(d) Categories of personal data

(e) Recipients or categories of recipients of the personal data, if any

(f) Existence of international transfer of personal data and the legal basis for that

(g) Period of personal data storage or the criteria to determine the period

(h) Rights of data subjects stipulated in Article 27

(i) Right to lodge a complaint with a supervisory authority

(j) Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract

(k) Whether the data subjects are obliged to provide the personal data

(l) Possible consequences of failure to provide the personal data

(m) Existence of automated decision-making

(2) When personal data is collected from a third person other than the data subject, in addition to the items stipulated in (1), our company shall also promptly provide the data subjects with the source of the personal data and whether it was from publicly accessible sources. However, in this case, it is not necessary to provide the data subjects with the items stipulated in (j) to (l) of (1).

(3) Other necessary information that are required by applicable laws and regulations shall also be included.

Article 20 (Requirements of consent)

(1) When personal data is to be collected based on the data subjects' consent, our company shall notify the data subjects of the items stipulated in (1) of Article 19 and obtain the consent from the data subjects with clear and plain descriptions prior to the collection.

(2) Our company shall keep a record of the consent obtained from data subjects for at least the period of the processing of personal data.

(3) When personal data of children is to be collected, the consent stipulated in (1) shall be obtained from the holders of parental responsibility.

Section 4 Personal Data Management

Article 21 (Records of processing activities)

Our company shall keep and update a record of the personal data processing activities including at least the following items at the initiation or changes of personal data processing.

(a) Registration date

(b) Personal data asset name

(c) Categories of personal data

(d) Quantity of personal data by each category of data subjects

(e) Total quantity of personal data

(f) Country / Area where the data subjects reside

(g) Method of collection

(h) Source of personal data

(i) Purpose of the processing

(j) Legal basis of the processing

(k) Managing personnel

(l) Form of data

(m) Storage place of personal data

(n) Security measures

(o) Period of personal data processing

(p) Period of personal data storage

(q) Confirmation of consent

(r) Accessible personnel

(s) Existence of joint control of personal data

(t) Existence of subcontracting of personal data

(u) Existence of disclosure of personal data to external organizations

(v) Existence of international transfer of personal data

(w) Disposal date

(x) Confirmation of disposal

Article 22 (Security management measures)

Our company shall implement appropriate security measures in accordance with separate rules in the collection, utilization, storage, transfer, erasure stages of the personal data.

Section 5 Personal Data Transfers

Article 23 (Subcontracting of personal data processing)

(1) Our company shall establish criteria for subcontractor selection and select subcontractors that have adequate personal data protection level when outsourcing the processing of personal data.

(2) Our company shall conclude contracts or addenda on personal data processing and manage and monitor the processing carried out by the subcontractors. Clauses that are required to be included by applicable laws and regulations shall be specified and included in the contracts or addenda.

Article 24 (Disclosure of personal data to external organizations)

When personal data is to be disclosed to external organizations, our company shall obtain the consent from data subjects prior to the disclosure.

Article 25 (Joint control of personal data)

When personal data is to be jointly controlled with external organizations, our company shall specify and document the obligations and responsibilities of both parties.

Article 26 (International transfer of personal data)

Our company shall not transfer personal data to individuals or organizations located in a third country or area in principle unless one of the following conditions is met.

(a) The supervisory authority in the origin country or area has determined adequate level of protection is ensured in the destination country or area.

(b) The origin and destination organizations have concluded a contract that ensures processing of personal data in the destination country or area to be carried out in compliance with the laws and regulations of the origin country or area.

(c) The data subjects have given consent to the international transfer.

(d) The international transfer is necessary for the performance or conclusion of a contract with the data subjects.

Section 6 Data Subject Rights

Article 27 (Response to data subject rights)

Our company shall respond promptly to the requests from data subjects based on the rights stipulated in Article 28 to Article 33 in accordance with the requirements stipulated in applicable laws and regulations.

Article 28 (Right to access)

Our company shall provide the data subjects with the following information upon data subjects' request based on the right of access.

(a) The purposes of the processing

(b) The categories of the personal data

(c) The recipients or categories of recipient to whom the personal data have been or will be disclosed, including recipients in third countries or areas

(d) The envisaged period for which the personal data will be stored, or the criteria used to determine that period

(e) The existence of the right to request rectification or erasure of the personal data or restriction of processing of the personal data concerning the data subjects or to object to such processing

(f) The right to lodge a complaint with a supervisory authority

(g) Where the personal data are not collected from the data subjects, any available information as to their source

(h) The existence of automated decision-making and the envisaged consequences of such processing for the data subjects

Article 29 (Right to rectification)

Our company shall rectify inaccurate personal data upon data subjects' request based on the right to rectification.

Article 30 (Right to erasure)

Our company shall erase personal data without undue delay upon data subjects' request based on the right to erasure where one of the following grounds applies.

(a) The personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed

(b) The data subject withdraws consent on which the processing is based, and where there is no other legal basis for the processing

(c) The data subject exercises the right stipulated in Article 33 and there is no overriding legal basis for the processing

(d) The personal data have been unlawfully processed

(e) The personal data have to be erased for compliance with a legal obligation of the company

Article 33 (Right to restriction of processing)

Our company shall consider stopping the processing of personal data upon data subjects' request based on the right to restriction of processing where one of the following grounds applies.

(a) The accuracy of the personal data is contested by the data subject for a period enabling the company to verify the accuracy of the personal data

(b) The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead

(c) The company no longer needs the personal data for the purpose of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims

(d) The data subject has exercised the right stipulated in Article 33 pending the verification whether the legal basis of the company override those of the data subject

Article 32 (Right to data portability)

Our company shall provide the data to the data subjects upon their request based on the right to data portability under both of the following conditions.

(a) The processing is based on the legal basis of "consent" or "performance of contract".

(b) The processing is carried out by a computer.

Article 33 (Right to object)

Our company shall discuss the appropriateness of the processing of personal data upon data subjects' objection when the processing is based on "legitimate interest" or "public interest" and respond accordingly.

Section 7 Education

Article 34 (Education)

Our company shall establish organizational structure for compliance with applicable laws and regulations and this rule and provide education to employees and other relevant personnel every 1 year.

Section 8 Document and Record Management of Personal Data Protection

Article 35 (Document and record management of personal data protection)

(1) Our company shall state in writing the following elements that are the base of the personal data management framework.

(a) Personal data protection policies

(b) Company rules

(c) Plans

(d) Records that are determined to be necessary for the implementation of personal data protection

(2) Our company shall establish, implement, and maintain procedures to manage all the personal data protection related documents including the following.

(a) Matters related to issuance and revision of the documents

(b) Clarification of correlation between the revisions and the versions of the documents

(c) Enabling easy reference to the documents as necessary

(3) Our company shall establish, implement, and maintain procedures to keep necessary records regarding personal data protection.

Chapter 5 Monitoring

Article 36 (Monitoring)

(1) Our company shall regularly monitor the compliance with applicable laws and regulations and this rule.

(2) Our company shall regularly check and update (inventory) the records of processing activities stipulated in Article 21. The results of such inventory shall be referred to and utilized for risk recognition, analysis and implementation of countermeasures stipulated in Article 11.

Chapter 6 Corrective Measures

Article 37 (Review of personal data management)

37.1 Our company shall establish, implement, and maintain procedures to assign the responsibility and authority to ensure the implementation of corrective and preventive measures against noncompliance. The procedures shall include the following.

(a) Check of the details of noncompliance

(b) Identification of the cause of noncompliance and planning of corrective and preventive measures

(c) Implementation of the planned measures within a predetermined deadline

(d) Keeping records of the result of the corrective and preventive measures that were implemented

(e) Review of the effectiveness of the corrective and preventive measures that were implemented

37.2 The President of our company shall review the personal data management framework at least once a year to maintain the protection level.

Chapter 7 Personal Data Incidents

Article 38 (Reporting criteria)

Our company shall clarify the classification of any incident related to personal data and criteria for reporting such incident occurrence to relevant departments of our company.

Article 39 (Reporting and response)

(1) Our company shall establish and maintain procedures to report to Mitsubishi Electric regarding any personal data incidents that have occurred.

(2) Our company shall establish and maintain procedures to discuss with Mitsubishi Electric and if applicable, report the incident to supervisory authorities or data subjects within the period required by applicable laws and regulations.

(3) Our company shall specify the items that shall be monitored and recorded, including the reason and cause of the incident, the details and the responses to the incident, etc. Our company shall establish and maintain procedures to record the items and to conduct final report to Mitsubishi Electric after completion of incident response.

MITSUBISHI ELECTRIC
Changes for the Better

MITSUBISHI ELECTRIC AUTOMATION (THAILAND) CO., LTD.
Bang-Chan Industrial Estate No. 111 Soi Serithai 54 T. Kannayao, A. Kannayao, Bangkok 10230 Thailand.
Tel: (66) 2517-1326, (66) 2919-9873 Fax : (66) 2517-1328 URL : www.meath-co.com E-mail : support_meath@meath.co.th
บริษัท มิตซูบิชิ อีเล็คทริค ออโตเมชั่น (ประเทศไทย) จำกัด
นิคมอุตสาหกรรมบางชัน เลขที่ 111 ซอยเสรีไทย 54 แขวงคันนายาว เขตคันนายาว กรุงเทพฯ 10230
โทรศัพท์ : (66) 2517-1326, (66) 2919-9873 โทรสาร : (66) 2517-1328 URL : www.meath-co.com E-mail : support_meath@meath.co.th

Chapter 8 Penalty

Article 40 (Penalty)

Employees who violate our company rules regarding the protection of personal data shall be subject to disciplinary punishment pursuant to the work regulations.

Article 41 (Contact)

A data subject can exercise your legal rights against the Company by using the form specified by the company and submit to the Personal Data Protection Officer: DPO

Contact address : No. 111 Soi Serithai 54, T.Kannayao, A.Kannayao, Bangkok 10230

E-mail : supakorn@meath.co.th Tel. 0-2517-1326 Ext. 222

This Privacy Policy is effective from March 20, 2023 onwards.

.....

(Mr. Somchin Leelaket)

President