

## PERSONAL DATA PROTECTION POLICY TotalEnergies Company in Thailand

Pursuant to the Personal Data Protection Act B.E. 2562 and other related laws, including any further amendments thereof (“**Personal Data Protection Laws**”), **TotalEnergies Company in Thailand**<sup>1</sup> (the “**Company**”) has made this Personal Data Protection Policy (“**Policy**”) to describe the details regarding the collection, use and disclosure of Personal Data to personnel and staffs of the Company in processing of Personal Data relating to the business operation of the Company, in accordance with the Personal Data Protection Laws.

### 1) DEFINITIONS

“**Personal Data**” means any information relating to a natural person, which enables the identification of such person, whether directly or indirectly, but not including the information of the deceased persons in particular.

“**Sensitive Personal Data**” means Personal Data consisting of information pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or any of the data which may cause unfair discrimination to the Data Subject or affect the Data Subject in the same manner as specified by Personal Data Protection Laws.

“**Data Subject**” means a natural person whose Personal Data identified to, such as customers, business partners, directors, Company’s personnel, visitors, and any other natural persons whose Personal Data are collected, used or disclosed by the Company.

“**Data Controller**” means a natural person or a juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of the Personal Data.

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

“**Process**”, “**Processes**”, “**Processed**” or “**Processing**” means any operation or set of operations towards Personal Data or set of Personal Data regardless of whether it conducts automatically, for instance, collection, recording, systematizing, structuring, preserving, rectifying or modifying, obtaining, determining, using; disclosing via sending, disseminating or any other actions which stimulate the readiness, composition or combination, constraint, erasure or destruction.

“**Legal Basis**” means the lawful grounds to collect and Process Personal Data as prescribed in the Personal Data Protection Laws.

### 2) LEGITIMACY OF PERSONAL DATA COLLECTION

The Company shall collect, use or Process Personal Data under a Legal Basis as specified in the Personal Data Protection Laws; whereby it is also stipulated as a guideline in this Policy as follows:

**2.1 General Personal Data:** The Company shall collect Personal Data under one or more of following legal basis as follows:

---

<sup>1</sup> **TotalEnergies Company in Thailand** means (1) TotalEnergies Marketing (Thailand) Co., Ltd. and/or (2) TotalEnergies Renewables (Thailand) Co., Ltd.

Legal Basis	Details
<b>(1) Vital Interest Basis</b>	The Company shall collect Personal Data where it is necessary to prevent or suppress danger to a person's life, body or health, which is not only limited to the Data Subject. For example, it is necessary for the Company to collect Personal Data in an emergency accident involving the Data Subject.
<b>(2) Contract Basis</b>	The Company shall collect Personal Data where it is necessary for the performance of a contract to which the Data Subject is a direct contracting party, or for certain proceedings under a request of the Data Subject before entering into the contract. For example, to entering into the contract or performing the contract executed between the Company and the job applicants, personnel, customers, business partners, or other contracting party or may be a contracting party with the Company, etc.
<b>(3) Public Interest Basis</b>	The Company shall collect Personal Data where it is necessary for carrying out the tasks for public interest of the Company, or exercising the duties empowered by official authority vested in the Company.
<b>(4) Legitimate Interest Basis</b>	<p>In some cases, the Company shall collect Personal Data from the Data Subject where it is necessary for the legitimate interests of the Company and/or any third parties, for example:</p> <ul style="list-style-type: none"> <li>- Processing Personal Data of the Job Applicants and Personnel for legitimate interests of the Company, Job Applicants and Personnel in consideration to employ the Job Applicant to be the Company's Personnel, including interests in human resource management of the Company</li> <li>- Processing Personal Data of the Clients, Business Partners of the Company for business communication with the Company's Clients, Business Partners, etc.</li> <li>- Processing Personal Data of the Personnel, visitors or any third party visiting the Company for monitoring and securing to life or properties of persons or the Company.</li> </ul> <p>However, the Company must act with caution when relying on this legal basis to collect Personal Data – as the Company may not collect Personal Data through relying on Legitimate Interest where such interests are overridden by the fundamental rights of the Data Subject, or where such interests may significantly affect the fundamental rights of the Data Subject. In such case, the Company must not collect Personal Data through relying on Legitimate Interest and is required to request for the Data Subject's consent if the Company intends to continue collecting his or her Personal Data.</p> <p>The following guideline is provided for implementing the legitimate interest basis. The Company must assess whether the collection of any Personal Data is in accordance with the following criteria in all respects:</p> <ul style="list-style-type: none"> <li>(a) Whether the Company or third party have legitimate interests to collect Personal Data or not;</li> <li>(b) Whether the collection of such Personal Data is necessary for the objective pursuant to Clause (a) or not;</li> <li>(c) Whether the Data Subject should expect that the Company is required to collect such Personal Data or not;</li> <li>(d) Whether the collection of such Personal Data is of no less importance than the fundamental rights of the Data Subject, or is not the case whereby the fundamental rights of the Data Subject is significantly affected or not; and</li> <li>(e) Whether the Company has appropriate Personal Data Protection measures in collecting Personal Data or not.</li> </ul>

Legal Basis	Details
<b>(5) Legal Obligation Basis</b>	The Company will collect, use or disclose Personal Data as required by laws. This may include processing Personal Data in accordance with court orders or government officials, for example, storing employees' personal data to comply with labor protection laws, storing accounting documents for a period specified by the laws, etc.
<b>(6) Consent Basis</b>	<p>Where Personal Data cannot be collected by means of any other legal basis as aforementioned in Clause (1)-(5), the Company will obtain a consent from the Data Subject <b>before or at the time</b> of collecting Personal Data. Consent shall be consisted or contemplated of the following details:</p> <ul style="list-style-type: none"> <li>✓ Made explicitly in writing or via electronic system, except where under certain circumstances such a request cannot be so made;</li> <li>✓ In requesting of consent from the Data Subject, it shall: <ul style="list-style-type: none"> <li>(i) state the purposes of collection, use, or disclosure of Personal Data;</li> <li>(ii) be clearly separated from other statements;</li> <li>(iii) be in a format or a statement which could be easily accessible and understandable, and the language used must be simple and not be deceiving or misleading the purposes of data collection to the Data Subject; and</li> <li>(iv) be concerned for the freedom of the Data Subject in giving such consent independently and voluntarily.</li> </ul> </li> <li>✓ The absence of a response or inaction is not regarded as consent from the Data Subject;</li> <li>✓ Data Subject may withdraw his or her consent at any time, unless there is a law or contract advantageous to the Data Subject which restricts the Data Subject's right to withdrawal;</li> </ul> <p>In case the Company shall request a consent from a minor, incompetent or quasi-incompetent person, the Company must obtain the consent from the holder of parental responsibility, the custodian or curator who has the power to act on behalf of such Data Subject subsequently. If the minor is above the age of ten years, they may give their own consent in the case where they can solely act by themselves under the applicable law.</p>

## 2.2 Sensitive Personal Data

The Company will collect, use or disclose such Sensitive Personal Data **only when the Data Subject has given his or her explicit consent** (please see guidelines and methods in Clause 2.1 (6)), except where the law provides that:

- it is for the purpose of prevention or suppression of danger to the life, body or health of a person, where the Data Subject is incapable of giving consent by whatever reason, often for emergencies;
- it is information that is disclosed to the public with the explicit consent of the Data Subject;
- it is necessary for an establishment of a legal right of claim, a compliance or an exercising of a legal right of claim, or a defense against a legal right of claim;
- it is necessary for compliance with the law to achieve the purposes with respect to:
  - preventive medicine or occupational medicine, the assessment of working capacity of the employee;
  - public interest in public health;
  - employment protection, social security, national health security, social health welfare of the entitled person by law or social protection in which the collection of Personal Data is necessary for exercising the rights or carrying out the obligations of the Company or the Data Subject;

- scientific, historical, or statistical research purposes, or other public interests; or
- other substantial public interest e.g. collecting sensitive Personal Data for the purpose of preventing contagious diseases or epidemic, collecting and disclosing sensitive Personal Data to government agencies to prevent money laundering.

Remark: The guideline for considering and interpreting ‘public interest’ may change according to the guidelines and the definition provided by the Personal Data Protection Committee or as specified in secondary legislation which may be promulgated in the future.

In any cases, details of the type, purposes, and legal basis for the collection of Personal Data by the Company will be specified in the Privacy Notice for different types of Data Subjects.

### **3) Guidance in Collecting of Personal Data**

The Company shall collect and Process Personal Data to the extent necessary to achieve the purposes stipulated by the Company and shall erase or destroy the data received without necessity, especially Sensitive Personal Data. For example, if the Company uses Personal Data to identify its business partner or their representative from a copy of the identification card, whereby typically the Company only requires general Personal Data for the identification of such person (i.e. name and photo). Hence, in case where the Sensitive Personal Data is contained in the identification card (i.e. religious beliefs and blood type), the Company should employ a method to prevent such Personal Data from appearing on the copy of the identification card when in the Company’s possession. This may include erasing unnecessary data received in the identification card, leaving only the necessary Personal Data for identification only.

This is for the purpose of mitigating the risks in unlawfully collecting, using and disclosing the Personal Data of the Company, and risks of leakage of Personal Data.

### **4) PRIVACY NOTICE FOR DATA SUBJECTS**

Upon collecting of Personal Data, the Company shall provide a Privacy Notice for various types of Data Subjects, such as job applicants, personnel and shareholders, customers, business partners or any individuals from which the Company will collect their Personal Data, to explain in details of collecting and Processing of Personal Data by the Company which the Privacy Notice shall at least include the following details:

1. Purpose of Personal Data Collection;
2. Lawful basis to Personal Data Collection;
3. Detailed information in case the Data Subject is required to provide Personal Data for compliance with the law or contract, or for entering into the contract, including the affect to Data Subject for not giving such required Personal Data;
4. Personal Data to be collected;
5. Retention period of Personal Data (in case definite period could not be determined, estimate period is required)
6. Categories of person or organization to which the Company discloses Personal Data;
7. Right of Data Subject;
8. Contact Information of the Company, such as address, contact method (The Company is required to provide the contact information of its agent or data protection officer, if any); and
9. Other related details for the Data Subject to be acknowledged, understood and taken into consideration to provide consent to the Company, in case the Company is unable to collect Personal Data without obtaining consent from the Data Subject.

The Company shall inform or deliver the Privacy Notice to the Data Subject before or at the time of collecting their Personal Data; except where the Company collects, uses or discloses the Personal Data prior to having this Policy, and it is still necessary for the Company to continually collect, use or disclose

that data, in such case, the Company shall inform or deliver the Privacy Notice to the Data Subject without delay.

The notification or delivery of the Privacy Notice may not be required to be repeated in the event that the Company has previously notified or delivered the Privacy Notice to such Data Subject. However, in the event that the Company revises the Privacy Notice, the Company must notify or deliver such revised Privacy Notice to the Data Subject.

## **5) SOURCE OF PERSONAL DATA**

In general, the Company will collect Personal Data from the Data Subject directly, for example, the Data Subject inform his/her Personal Data to the Company in verbal or send the documents containing his/her Personal Data to the Company, etc.

However, if the Company is necessary to collect Personal Data from other sources which is not directly from the Data Subject, the Company shall (i) inform the Data Subject of such collection along with the Privacy Notice without delay but shall not exceed 30 days upon the date of such collection; and (ii) obtain a consent from the Data Subject in the case of collecting Personal Data under the consent legal basis. Notwithstanding, except in the case the Company is required to use the Personal Data to contact the Data Subject, the Company shall inform the Data Subject upon the first communication with the Data Subject. In case of disclosing Personal Data, the Company shall inform the Data Subject prior to the first disclosure.

In some cases, the Company may not be required to execute clause (i) if the Company can prove that such notice is not possible, or will obstruct the use or disclosure of the Personal Data, or the Data Subject is already aware of such detailed information. For example, the Data Subject has received the Privacy Notice for other business transactions with the Company and intends to carry out the same transaction with the Company again.

In addition, if the Company hires the Data Processor to collect, use or disclose Personal Data on behalf of and by order of the Company, the Company may assign the Data Processor to provide privacy notices on its behalf whereby the Company is required to make sure that the Data Processor complies with and performs the obligations as stated in this Policy and it shall be deemed that the Company has provided the details of collection, use and disclosure of Personal Data in compliance with the Personal Data Protection Laws as the Data Controller.

## **6) RIGHTS OF THE DATA SUBJECT**

The Company shall be aware that the Data Subject has the right to take any actions regarding his/her Personal Data in the Company's possession as stipulated in the Personal Data Protection Laws. Thus, the Company shall provide a Data Subject Request Form to facilitate and enable the Data Subject in notifying his/her intention to exercise his/her rights. However, in the event the Company has any reasonable ground to reject the Data Subject's request, the Company shall notify the Data Subject of such rejection in writing.

<b>Data Subject's Right</b>	<b>Details</b>
<b>6.1 Right to withdraw consent</b>	Data Subject may withdraw some or all of his or her consent, which was previously given to the Company through the Consent Letter, at any time throughout the period the Company retains the Personal Data. The Company must also notify the Data Subject of any effects or consequences (if any) the withdrawal of consent will have on the Data Subject. Notwithstanding, the withdrawal of consent shall not affect the processing of Personal Data by the Company that the Data Subject has already given consent prior to the withdrawal.

Data Subject's Right	Details
	<p><b>Rejection Reason:</b> Restrictions on the right to withdraw consent includes legal compliance or contract performance which is beneficial towards the Data Subject.</p> <p><b>Response time:</b> Without delay.</p>
<p><b>6.2 Right to request access to and obtain a copy of the Personal Data</b></p>	<p>Data Subject is entitled to request access to and obtain a copy of the Personal Data related to him or her which is in responsibility of the Company, or to request the Company to reveal how the Company obtained the Personal Data without his or her consent.</p> <p><b>Rejection Reason:</b> The Company may reject the Data Subject's request only in the following cases:</p> <ul style="list-style-type: none"> <li>- To comply with a legal obligation or court order; or</li> <li>- The Company opines that fulfilling the Data Subject's request will override the fundamental rights and freedoms of other persons.</li> </ul> <p>However, in case of any rejection to the Data Subject's request of his or her rights as stated above, the Company shall keep a record of such rejection together with the reasons thereof.</p> <p><b>Response time:</b> Where such requests cannot be rejected, the Company shall comply with the request of the Data Subject within 30 days of receiving the request.</p>
<p><b>6.3 Right to request to receive and send or transfer of Personal Data</b></p>	<p>Data Subject has the right to request obtaining his or her Personal Data from the Company, or to request the Company to send or transfer the Personal Data to another person or organization in a format which is readable or commonly used. This includes the right to receive his or her Personal Data which are transferred and maintained by other companies, personnel or organizations. This request can only be used if the Personal Data has been collected, used or disclosed with consent, or for contract performance or for precontractual request between Data Subject and the Company.</p> <p><b>Rejection Reason:</b> The Company can refuse the Data Subject's request in sending or transferring Personal Data which is used for the performance of a task carried out for the public interest, or for compliance with the law, or such exercise of rights shall violate the rights and freedoms of others. For example, the integral part of the information contains trade secrets or intellectual property information attached to the Personal Data.</p> <p>However, in case of any rejection reason to the Data Subject's request of his or her right as stated above, the Company shall keep a record of such rejection together with the reasons thereof.</p> <p><b>Response time:</b> Without delay.</p>
<p><b>6.4 Right to object the collection, use, or disclosure of the Personal Data</b></p>	<p>Data Subject has the right to object to the collection, use or disclosure of their Personal Data by the Company in the following circumstances:</p> <ol style="list-style-type: none"> <li>(1) Collection, use or disclosure of such Personal Data is carried out for the performance of a task necessary for legitimate interests, or carried out in the public interest, including complying with orders of government officials.</li> </ol> <p><b>Rejection Reason ( for Clause 6. 4( 1 ) ) :</b> The Company can demonstrate that there is a more compelling legitimate ground than the interests, rights, or freedom of the Data Subject, or the data collection, use or disclosure is carried out for the establishment, compliance or exercise of legal claims, or defense of legal claims.</p> <p>However, in the event of denying the Data Subject's request of his or her Personal Data rights as stated above, the Company shall keep a record of such denial together with the reasons thereof.</p> <ol style="list-style-type: none"> <li>(2) For the purpose of direct marketing, the Data Subject can object without any conditions.</li> <li>(3) For the purpose of scientific, historical or statistic research, unless it is necessary for performance of a task carried out for the public interest.</li> </ol> <p><b>Response time:</b> Without delay. In the case the Company does not have a reason for the denial of such request, the Company shall immediately</p>

Data Subject's Right	Details
	proceed to separate the Personal Data out from other data immediately upon the notification of the Data Subject's objection.
<b>6.5 Right to erase the Personal Data</b>	<p>Data Subject has the right to request the Company to erase or destroy the Personal Data, or anonymize the Personal Data to become anonymous data which cannot identify the Data Subject or cannot be further reused, where the following grounds applies:</p> <ol style="list-style-type: none"> <li>(1) The Personal Data is no longer necessary to be retained for the purposes for which it was collected, used or disclosed; whereby in relation to the period where it is applicable to notify the Data Subjects in the Privacy Notice;</li> <li>(2) The Data Subject withdraws consent, and where the Data Controller has no other legal grounds for such collection, use, or disclosure;</li> <li>(3) The Data Subject objects to the collection, use, or disclosure of the Personal Data, and the Company cannot reject to such request; or</li> <li>(4) The Personal Data has been unlawfully collected, used, or disclosed.</li> </ol> <p><b>Reason for denial:</b> The Company is entitled to reject the request in case of collection, use, or disclosure of Personal Data in the following cases:</p> <ul style="list-style-type: none"> <li>- Storing for the purpose of freedom of expression;</li> <li>- To achieve the purpose relating to the preparation of historical documents, or archives of research, statistics or for public interests;</li> <li>- The collection of Sensitive Personal Data which is necessary for compliance with the law to achieve the purposes with respect to preventive medicine or occupational medicine, the assessment of working capacity of the employee or public interest in public health;</li> <li>- For the purpose of establishment, compliance or exercise of legal claims, or defense of legal claims;</li> <li>- For compliance with the law.</li> </ul> <p>Where the Company has disclosed the Personal Data to the public or transferred to other Data Controllers, and the Data Subject has requested for his or her Personal Data to be erased, destroyed, or anonymized, the Company shall proceed to have such Personal Data erased or destroyed, or anonymized. In addition, the Company shall inform other Data Controllers to proceed in the same manner. The Company shall be responsible for the expenses concerning the erasure or destroying and informing as aforesaid.</p> <p><b>Response time:</b> Without delay.</p>
<b>6.6 Right to restrict the use of the Personal Data</b>	<p>Data Subject may request the Company to restrict the use of the Personal Data in the following circumstances:</p> <ol style="list-style-type: none"> <li>(1) There has been a request to correct Personal Data whilst the Company is pending the examination process of the request. However, the Company may consider denying the request to restrict the use of their Personal Data if after examination, the Company finds that the Personal Data is accurate, and the Company notifies the Data Subject of the reason prior to rejecting their request;</li> <li>(2) When the Personal Data has been processed unlawfully and the Data Subject had requested for restriction instead of deletion of such data;</li> <li>(3) When it is no longer necessary to retain the Personal Data, but the Data Subject has to request the Company to retain such data for the purposes of the establishment, compliance, or exercise of legal claims, or the defense of legal claims; or</li> <li>(4) The Company is pending the verification to object the processing of Personal Data. However, the Company may reject the Data Subject's request to restrict the use of their Personal Data if the Company has grounds on denial to the right to object as stated above.</li> </ol> <p><b>Response time:</b> Without delay.</p>
<b>6.7 Right to rectification</b>	<p>Data Subject may request the Company to ensure that their Personal Data remains accurate, up-to-date, complete, and not misleading.</p>

Data Subject's Right	Details
	<p>However, in case any of rejection reason to the Data Subject's request of his or her rights as stated above, the Company shall keep a record of such rejection together with the reasons thereof.</p> <p><b>Response time:</b> Without delay.</p>
<p><b>6.8 Right to file a complaint</b></p>	<p>Data Subject has the right to file a complaint to the expert committee as appointed by the Personal Data Protection Committee in the event that the Company or the Data Processor, including the employees or the service providers of the Company or the Data Processor violates or does not comply with the Personal Data Protection Laws.</p>

## 7) DUTIES AND RESPONSIBILITIES OF PERSONNEL

All staffs and personnel, including all employees and person hired by the Company are responsible for complying with the laws and this Personal Data Protection Policy and must keep Personal Data strictly confidential and must not use Personal Data received during working as an employee for any inappropriate, personal interest or illegal purposes. The duties of the personnel may be sorted by rank of position as follows:

### 7.1 The managing director and upper management level

Shall be responsible for overseeing all the Company's process to protect Personal Data as follows:

- Designate a person or department responsible for overseeing and handling all matters relating to Personal Data protection from all departments within the Company;
- Assign employees the responsibility to identify the procedures regarding Personal Data protection, including risk management procedures which may arise from the collection, use and disclosure of Personal Data by the Company, together with the practical guidelines in the event of a data protection violation within the Company;
- Implement control and monitoring of compliance with this Policy, including assessing the suitability of this Policy on a regular basis;
- Approve the process of the Policies concerning Personal Data protection, for example ensuring the suitability of this Policy, how Personal Data is protected within the Company, or amendment of this Policy; and
- Consider and approve requests of the Data Subject to exercise his or her rights concerning his or her Personal Data in cases where their request may have a significant impact towards the Company, Data Subject and/or other persons.

### 7.2 Designated persons responsible for the Personal Data Protection of the Company

Shall be responsible for advising and reviewing all of the Company's Personal Data protection processes as follows:

- Analyze, evaluate, audit and control the Company's Personal Data processing activities and advise personnel or other departments within the Company to ensure the Company's Personal Data processing activities comply with the Personal Data Protection Laws and the Company's Personal Data Protection Policy;
- Review and approve Personal Data protection practices of each department within the Company. This shall include practices to manage risks that may arise from the collection, use and disclosure of Personal Data by the Company and methods to solve situations of Personal Data breach occurring within the Company;
- Analyze, evaluate and advise personnel and departments within the Company on how to respond to the Data Subject's request to exercise his/her right in cases where their request may have a significant impact towards the Company, Data Subject and/or other persons;



- Report incidents regarding Personal Data processes within the Company to the managing director and executive personnel;
- Contact, coordinate and cooperate with the Office of the Personal Data Protection Committee, including proceedings concerning incidents of Personal Data breaches occurring within the Company, within the period specified by law.
- Study the details of the Personal Data Protection Act B.E. 2562 (2019), rules, announcements, orders, regulations or other laws relating to Personal Data protection. This shall include to follow up on amendments or revisions of laws relating to the protection of such Personal Data and to notify the Company's personnel; and
- Explain, create an understanding and awareness to the Company's personnel on Personal Data protection and relevant Personal Data protection laws.

### **7.3 Department manager level**

Shall be responsible for supervising the collection, use or disclosure of Personal Data within their department, which may have different characteristics in each department. The responsibilities may be categorized as follows:

- Allow any person to access Personal Data or assign the responsibility to an employee to manage the Personal Data within the department;
- Provide guidelines and training for Personal Data in the department and ensure that all members of staff in the department understand Personal Data which is required to be collected and Personal Data which is not necessary to collect for the operation of the department;
- Provide standardized measures to secure Personal Data in the department in accordance with the law and this policy;
- Approve responses of Data Subject's requests to exercise his or her rights and consult with relevant departments, including consulting with the designated persons responsible for the Personal Data protection of the Company and reporting to management to request for their approval if the request may have a significant impact towards the Company, Data Subject and/or other personnel;
- Consult with management and designated persons responsible for the Personal Data protection to determine appropriate Personal Data protection practices;
- Provide a record of the collection, use or disclosure of Personal Data of the department in accordance with the lists specified herein this Policy; and
- Keep a report of all Personal Data breaches from the contolees and consider whether such breach will affect the rights and freedoms of the Data Subject, including consulting with the designated persons responsible for the Personal Data protection of the Company and management to consider whether any appropriate action needs to be taken in accordance with this Policy.

### **7.4 Staff level**

Shall act strictly in accordance with the laws and this Policy to protect Personal Data, in particular the following steps:

- Collect, use and disclose Personal Data in accordance with the law and this Policy, including participating in training regarding Personal Data protection of the Company;
- Perform duties assigned to protect Personal Data while handling Personal Data, for example the security, transmission, disclosure or recording Personal Data etc.;
- Inform supervisors when the collection, use or disclosure of Personal Data in the Company or any action they were instructed is unlawful. In addition, to further inform supervisors when the collection, use or disclosure of any Personal Data may pose a risk of violation to the fundamental rights and freedoms of Data Subjects;
- Notify the supervisor to approve any Data Subject's requests to exercise their rights; and
- Notify the supervisor immediately if they become aware of any Personal Data privacy breach, whether it is a deliberate misconduct or negligence of any party whatsoever and whether the breach may pose a risk of violating the fundamental rights and freedoms of Data Subjects.

**Remark:**

Violations of the Personal Data Protection Laws and/or this Policy by personnel may result in disciplinary action and if such violation or non-compliance results in damage to the Company, the Company reserves the right to terminate the employment or agreement. In addition, there may be criminal penalties, fines and imprisonment for the Company's representative who breaches or fails to comply with the law. Thus, employees and related parties should review and strictly adhere to the Personal Data Protection Laws and this Policy.

**8) DUTIES AND RESPONSIBILITIES OF DATA PROCESSOR**

In case the Company engages or assigns the Business Partner to perform any of the actions to the Company which such action is operated upon the Personal Data and such Business Partner is considered as a Data Processor of the Company who conducts by the order or on behalf of the Company, the Company shall execute the Data Processing Agreement and stipulate that the Data Processor shall act strictly in accordance with the laws and this Policy with the following responsibilities:

- Collect, use and disclose Personal Data in accordance with the law and this Policy and within the purposes or instructions of the Company as specified in the Data Processing Agreement, including participating in the training session regarding Personal Data protection of the Company upon request;
- Arrange for appropriate security measures to prevent loss, access, use, modification, amendment, or disclosure of Personal Data without authorization or illegitimately, and notify the Company of any violation of Personal Data.
- Notify the Company without delay and within 24 hours if there is any violation of Personal Data so arisen from the moment of becoming aware of such violation; and
- Support and assist the Company in responding to the Data Subject's request in exercising their rights.

**Remark:** Any violations of the Personal Data Protection Laws or this Policy by the Business Partner which is a Data Processor of the Company may be regarded as a breach of contract with the Company. If such violation or non-compliance results in damage to the Company, the Company reserves the right to terminate the contract.

**9) PERSONAL DATA PROTECTION MEASURES**

The Company must provide appropriate security measures on handling Personal Data, in administrative, technical and physical safeguard regarding the access control of Personal Data, with at least the following actions:

- (1) Controlling access to Personal Data and devices for storing and Processing Personal Data with regard to usage and security;
- (2) Determination of permission or right to access Personal Data;
- (3) User access management to control the access of Personal Data only for authorized persons;
- (4) Determination of user responsibilities to prevent unauthorized access to Personal Data, disclosure, knowing or illegal copying of Personal Data, theft of Personal Data storage or Processing equipment;
- (5) Measures to enable retrospective review of access, change, deletion or transfer of Personal Data in accordance with the methods and devices used for collecting, using or disclosing Personal Data.

Nevertheless, the Company shall further review such measures when it is necessary or when there is any technology advancement to ensure that Personal Data is treated in a secure manner and in accordance with the standards prescribed by the laws.

## **10) RECORD OF PERSONAL DATA PROCESSING**

The Company shall have a record of Personal Data Collecting and Processing activities which shall consist of, at the very least:

- The lists of the collected Personal Data with the objectives and the retention periods,
- The usage or disclosure of Personal Data under the legal basis other than consent,
- The rights, method and condition for exercising of rights to access the information of the Data Subject,
- Rejection or objection of request to exercise the rights, including the reasons as defined herein this Policy, and
- The explanation of security measures which the Company has prepared.

This is for the purpose that the Data Subject can examine and enforce their rights where the Data Subject has notified or requested to the Company.

## **11) DISCLOSING, SENDING OR TRANSFERRING PERSONAL DATA TO OVERSEA**

The Company is able to send or transfer Personal Data to foreign countries or international organization limited to the following circumstances:

11.1 The destination country or international organization that receives such Personal Data has adequate data protection standards.

11.2 In the event the Personal Data protection standard of a destination country or international organization is inadequate, the transfer of Personal Data shall be carried out in accordance with the following:

- it is for the compliance under the laws;
- consent of the Data Subject has been obtained, provided that the Data Subject has been informed of the inadequate Personal Data protection standards of the destination country or international organization;
- it is necessary for the performance of a contract to which the Data Subject is a party, or for the precontractual request of the Data Subject;
- it is proceeding under the contract between the Company and other persons or juristic persons for the interests of the Data Subject;
- it is to prevent or suppress danger to the life, body, or health of the Data Subject or other persons, when the Data Subject is incapable of giving the consent at such time; or
- it is necessary for carrying out the activities in relation to substantial public interest.

11.3 The Company may send or transfer Personal Data to another person or juristic person in a foreign country and within the same group/affiliated Company without having to proceed with the prior specification in Clause 11.1. and 11.2. above. Notwithstanding, the Company has to put in place the Personal Data protection policy regarding sending or transferring Personal Data within the group/affiliated companies, and such policy has been reviewed and certified by the Office of the Personal Data Protection Committee (no policy on data portability has been established among the group/affiliated Company at present).

Currently, the Personal Data Protection Committee has not yet established a list of countries with sufficient standards nor adopted certification policies for sending or transferring the data within the group/affiliated companies. However, the Company is entitled to send or transfer Personal Data to foreign countries or international organizations if the Company has appropriate security measures of Personal Data which enable the enforcement of the rights exercised by the Data Subjects, including having effective legal remedies in accordance with the standards prescribed by the law. Notwithstanding, as the laws have not prescribed such measure, the Company is able to proceed on

the sending or transferring of Personal Data to be in accordance with Clause 11.2 until the law relating to such matter is a further promulgated.

## **12) HANDLING OF PERSONAL DATA BREACH**

Upon the breach of Personal Data incurred within the Company, employees and personnel shall coordinate to investigate and find solutions in order to avoid the same violation incident. Whereby, the Company is obliged to notify the breach to the Office of the Personal Data Protection Committee without delay and **within 72 hours** after having become aware of it and to the possible extent. In the event where such violation has a high risk to cause an effect towards the right and liberty of the Data Subject, the Company must inform the breach incident to such Data Subject and the remedy measures without delay.

## **13) AMENDMENT OF PERSONAL DATA PROTECTION POLICY**

This Personal Data Protection Policy will be amended and rectified as appropriate, subject to the amendment of laws and the appropriateness of business.

This Policy has recently been revised on [Please specify].

## **14) CONTACT INFORMATION**

Any question regarding personal data protection or in the event that you would like to report a violation of Personal Data, please contact:

Data Protection Division

**TotalEnergies Marketing (Thailand) Co., Ltd.**

173/5 Asia Centre Building, 12<sup>th</sup> Fl.

South Sathorn Road, Thungmahamek,

Sathorn, Bangkok 10120

02 – 1636364

dpth@totalenergies.com