PTG ENERGY GROUP

Supporting Document

on

Personal Data Protection Policy

Record of Revisions

Rev No.	Execution Date	Description
03	01/01/2024	Revise all documents
02	23/09/2022	Modify The Duration of Consideration and Notification of Results to The Users
01	13/05/2021	2021 Annual Review
00	01/03/2021	First Execution

Personal Data Protection Policy

PTG Energy Public Company Limited and its subsidiaries ("**the Group**") emphasize and respect the privacy and awareness of personal data protection, including maintaining the security of personal data in compliance with the law and international standards.

The Group has therefore announced this Personal Data Protection Policy ("**Policy**") with the objectives to notify details of personal data protection and management to maintain security of personal data as customers, trading partners, contractors, present, past and potential future customers or corporate trading partners, employees, personnel, officers, representatives, agents, authorized persons to act on behalf of juristic persons, directors, contacts and other natural persons acting on behalf of juristic persons which are customers or corporate trading partners of the group of companies, shareholders, investors and other relevant persons; to ensure that any personal data collected, used, disclosed or transferred to local and/or overseas third parties by the group of companies is protected and complies with personal data protection law.

In the case where the data subject is a member customer of PTT Max Card, further details can be found in the Privacy Policy announcement on the website:
https://www.maxcard.co.th/PrivacyPolicy.htm

In addition, the Group has defined privacy settings for cases where personal data is collected and used from accessing the websites of the Group. The Group will implement security measures to ensure the security of personal data according to appropriate measures.

Scope of Application

This policy applies only to the collection, use or disclosure of personal data by PTG Energy Company Limited (Public Company) and its subsidiaries, which operate any businesses not regulated by the Bank of Thailand. All existing policies, rules, regulations, orders, guidelines, announcements and requirements shall remain in effect to the extent that they do not conflict or contradict this policy.

Definitions

"Personal data" refers to information about an individual that can directly or indirectly identify that individual, except for the data of deceased individuals, which the Group has collected, used, and disclosed as stated in this policy.

"Sensitive personal data" refers to personal data which the Personal Data Protection Act B.E. 2019 ("Personal Data Protection Law") defines as sensitive that the Group has collected, used, disclosed, or transferred to outside parties and/or abroad when the Group has obtained explicit consent from the data subject. Sensitive personal data includes data concerning racial, ethnic origin, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disabilities, labor union information, genetic data, biometric data or any other data which affects the data subject in a similar manner, etc., including other data as specified in the announcement of the Personal Data Protection Committee.

"Health data" refers to personal information related to health or medical data.

"Personal Data Owner" refers to a natural person who owns the personal data that the Group collects, uses or discloses, such as customers, business partners, contractual parties, employees, workers, personnel, officers, representatives, authorized persons, representatives acting on behalf of a juristic person, directors, contacts, and other natural persons acting on behalf of a juristic person who are customers or business partners of the Group, shareholders, investors, visitors or users of websites, applications, devices or other communication channels, and other persons associated with the Group.

"Data controller" refers to an individual or legal entity with the authority to make decisions regarding the collection, use, or disclosure of personal information.

"Personal data processor" refers to an individual or legal entity that processes, uses, or discloses personal information on behalf of or under the instructions of the data controller. It should be noted that such individuals are not the data controllers themselves.

"Personal Data Protection Officer" refers to an individual or legal entity responsible for overseeing, providing advice, and monitoring the activities of the data controller and personal data processor. Additionally, they serve as a coordinator to collaborate with the Office.

"Consent" means the intentional expression of the personal data owner to permit the collection, use, or disclosure of their personal information. This expression may be in written or electronic form, unless obtaining consent in such a manner is not possible under the circumstances.

"Privacy Notice" means detailed information for notifying the data subject about the collection, use, or disclosure of personal information, including the management of personal data, the rights of the data subject, the duration of personal data retention, the destruction of personal data, and the contact channels for the Data Protection Officer.

"Rights of the data subject" refer to the rights of the data subject in managing their personal data, such as the right to access personal information, the right to request the sending or transfer of their personal data to others, the right to object, the right to disclose the sources of their personal data, the right to delete, destroy, or suspend the use of their personal data, and the right to ensure that their data is up-to-date.

"Leakage of personal data" refers to the unauthorized disclosure, breach, or violation of security measures for personal information, resulting in damage, loss, alteration, or disclosure without permission.

"Office" refers to the Office of the Personal Data Protection Committee, responsible for managing the protection of personal data, conducting academic and administrative work for the committee. The Secretary-General of the Office of the Personal Data Protection Committee serves as the executive in charge of the office's operations.

Roles, Responsibilities, and Accountability:

1. **The Board of Directors** is responsible for supporting and promoting the operations of the Group in compliance with laws, regulations, rules, directives, announcements, measures, and various practices, including customs, professional standards, ethics, and related codes of conduct relevant to the business operations of the Group.

2. **The Corporate Governance Committee** is tasked with providing support and assistance to the Board of Directors in overseeing the Group's operations, ensuring compliance with laws, regulations, rules, directives, standards, and applicable practices governing the business operations of the Group. This is achieved by establishing policies and appropriate operational procedures suitable for the business operations of the Group, including guidelines for ethical business oversight practices.

3. Risk Management Committee

3.1 Evaluate the effectiveness of compliance with the personal data protection policy of the Group and report the assessment results to the company's committee regularly, at least once a year. Also, ensure oversight to ensure that various risks related to personal data are managed, and appropriate risk management guidelines are in place.

3.2 Establish and review operational standards and practices to ensure that the operations of the Group comply with laws and the personal data protection policy of the Group.

3.3 Appoint officers responsible for the protection of personal data within the Group.

4. The Group's internal group committee is responsible for understanding and enforcing policies related to the protection of personal data, and overseeing that all employees within its company adhere strictly to these policies.

5. Senior-level executives are tasked with reviewing and approving orders, announcements, guidelines, or internal practices within their respective departments. They are also responsible for supervising employees and contractors within their units to ensure accurate and compliant implementation of personal data protection tasks in accordance with the policies, operational regulations, orders, announcements, or internal practices of their departments.

6. Compliance Division:

6. 1 Summarize the key information regarding changes or new enforceable announcements related to the data protection laws that impact the business operations of the Group. This information should be communicated to the board of directors, executives, employees, and data protection offices to ensure accurate and complete compliance with laws, regulations, and good corporate governance principles.

6. 2 Oversee the establishment of rules, regulations, policies, and relevant operating manuals to ensure compliance with internal regulations within the Group. This includes actively participating in the creation, review, amendment, and improvement of rules, regulations, policies, and operating manuals.

6.3 Participate in and provide input for the development, review, amendment, and improvement of rules, regulations, policies, and operating manuals related to data protection within the Group. Additionally, monitor and assess compliance with laws and regulations, offering suggestions and recommendations to internal departments within the Group for legal compliance in data protection matters.

7. Risk management division is responsible for overseeing and controlling compliance with standards in risk management practices. This includes assessing the efficiency and adequacy of risk management practices in accordance with the necessary and appropriate criteria. The division provides recommendations to the risk management committee and executives regarding operational practices necessary to prevent or mitigate risks that may arise from non-compliance with standards.

8. Internal Audit Division

8. 1 Set objectives and directions for the internal audit mission to support management and operations in complying with personal data protection laws. Consider the efficiency of risk management

and adequacy of the Group's internal control system.

8.2 Audit compliance with personal data protection standards within the Group, within the scope of internal audit work, in accordance with internal audit standards, ethical principles of internal auditors, and guidelines or practices of internal auditing according to international standards.

8. 3 Review process documents and assess the effectiveness of maintaining the security of systems related to personal data.

8.4 Report audit inspection results to the audit committee of the Group.

9. Information Technology Division are responsible for providing support and managing efficient information technology systems appropriately, adequately, and in accordance with the principles and regulations of the law applied in the process of personal data protection or internal operations of relevant division. This is to facilitate operational activities and promote accurate compliance with the principles and regulations of the law regarding personal data protection.

10. Legal Division are responsible for considering the modification, addition, or clarification of contracts or agreements within the Group and agreements between the Group and clients or business transaction counterparts, directors, executives, employees, contractors, as well as business partners, external service providers, and business partners. They are tasked with managing personal data in accordance with the laws governing personal data protection, providing advice or additional opinions on compliance with personal data protection laws when requested by the relevant division.

11. Assurance and Quality System Management Division are responsible for providing support and emphasizing compliance with standards by jointly reviewing and verifying efficiency, suitability, adequacy, and correctness according to the principles of laws, regulations, rules, orders, announcements, measures, practices, professional standards, ethics, and customs related to personal data protection within the business operations and information technology systems of the Group.

12. Human Resources Development Division is responsible for providing support and managing training on knowledge for all new employees. It also conducts refresher training for current employees, especially for division related to ensuring understanding and compliance with laws related to personal data protection, policies, operational regulations, orders, announcements, practices, or guidelines concerning the organization's personal data protection. Records of employees' training history must be maintained as evidence, and employees must undergo training when it is due for knowledge review. Additionally, it is necessary to manage the personal data of board members, executives, employees, and contractors of the Group under the responsibility of the division to comply with the measures for protecting the security of personal data.

13. Personal Data Protection Office:

13. 1 Supervise the establishment of a personal data governance structure and internal controls within the Group to ensure compliance with laws and the personal data protection policies of the Group.

13.2 Oversee and support the Group in implementing effective personal data protection measures in accordance with the law.

13. 3 Establish a structure for monitoring personal data and internal controls, including incident response practices, to promptly identify and manage abnormal events related to personal data breaches or leaks.

13. 4 Supervise employees, relevant divisions and departments, and the Group to ensure compliance with policies regarding personal data protection, internal regulations, orders, announcements, practices, or internal operation manuals within the organization, related to strict compliance with personal data protection.

13. 5 Communicate policies and relevant regulations regarding personal data protection that are newly announced or revised, modified, or amended to employees and related divisions and departments within the Group for acknowledgment and compliance.

13.6 Serve as the coordinating unit with the Office.

13. 7 Provide advice on standards and operational practices, including knowledge training on personal data protection, to employees and related divisions and departments within the Group.

14. Executives and Employees:

14. 1 Prioritize and adhere strictly to the laws concerning the protection of personal data, the Group policies, regulations, orders, announcements, guidelines, or operational manuals related to the strict protection of personal data.

14. 2 Attend knowledge training sessions on personal data protection as per the scheduled training program. When notified to attend training, emphasize the importance and actively participate in the training sessions with diligence.

14.3 Report cases of unauthorized personal data breaches promptly to the department head for joint verification of the transaction's accuracy. Inform the Personal Data Protection Office immediately upon discovery of the incident to comply with the specified time frame.

14. 4 Refrain from disclosing personal data of the data owner, which one becomes aware of or acquires through work activities, except as required by law.

Personal Data Collected by The Group

Personal data collected, used, or disclosed by the Group includes, but is not limited to, the following types of personal data:

(1) Personal information such as name, surname, title, national identification card number, passport number, taxpayer identification number, position, nationality, age, and sensitive information visible on a copy of the national identification card, such as religion, ethnicity, and blood type. The Group obtains explicit consent from the data owner or processes such information as necessary under applicable laws.

(2) Contact information such as address, telephone number, mobile phone number, and email.

(3) Financial information such as bank account numbers, transaction details, and credit card numbers.

(4) Other personal information such as data related to the use of information systems and the Group websites, recording images from closed-circuit cameras, and recording conversation audio.

(5) Health information, including data or records related to medical history, physical examinations, laboratory results, radiographic results, and other health-related information.

(6) Health information of service users recorded by healthcare professionals or consultants through the application, including, but not limited to, medical records, information about medical examinations, weight, height, symptoms, chronic illnesses, prescribed medications, allergic reactions, surgical history, blood pressure, pulse rate, body temperature, vision values, additional recommendations from healthcare professionals, prescribed medications, and other health- related information for all service users.

In case the owner of personal data is a minor under the age of 10, a person with disabilities, or an incapacitated person, the Group requests that the legal guardian or appointed guardian, according to the law of the owner of the personal data, act on behalf of the owner of the personal data and provide consent to the Group. Additionally, if the Group discovers that personal data has been collected without legal consent from the legal guardian or appointed guardian under the mentioned conditions, the Group rejects any requests from the owner of the personal data and will promptly delete the personal data unless the processing of such personal data is allowed by law, as specified by the data protection laws.

Furthermore, the Group has also collected, used, and disclosed sensitive personal information, such as facial recognition and fingerprint data. The Group has obtained explicit consent from the owner of the personal data or carried out such processing as necessary and permitted by law.

The Source of Personal Data

The Group may collect personal data from individuals who provide such information to the Group, whether through channels related to the purchase or exchange of goods and services, exchanging business cards, providing information through various electronic channels, or receiving personal data from other sources, such as product sales representatives or related service providers, government agencies, companies within the Group, and so on.

Additionally, the Group may also collect, use, and disclose sensitive personal information, including facial recognition and fingerprint data, with explicit consent from the individuals or as necessary according to applicable laws.

Purposes of Processing Personal Data

The Group processes personal data collected for the following purposes:

(1) Necessary for business transactions, fulfillment of contracts, or consideration of requests from the data subject before entering into an agreement. Examples include communication for buying and selling goods and services, contract execution, actions related to collection or payment of goods or services, consideration for procurement, delivery or receipt of goods or services, payment of

compensation, performance of duties according to positions, examination, and monitoring of work performance under the contract, and so on.

(2) For legal benefits such as verification of accuracy or quality of goods or services according to international standards, investigation or confirmation of facts, or for preventing, controlling, or investigating fraudulent activities, or for security, legal tax or accounting consultation, and so on.

(3) To comply with laws related to business operations or business activities, such as providing information to government agencies as required by law, compliance with court orders or orders of legal officers, operations related to licensing or issuance of permits under the law, payment of fees according to the law, establishment or exercise of legal rights or claims in court, organization of meetings, and payment of compensation as entitled by the data subject according to the law.

(4) For analyzing the use of products or services by members, organizing promotions, or providing discounts on goods or services to meet preferences.

In addition, upon obtaining consent from the owner of personal data, the Group may collect and use personal information for marketing purposes. This includes providing the owner of personal data with benefits such as sending newsletters, advertisements, organizing campaigns, conducting sales and marketing activities, delivering promotions, privileges, or discounts, or inviting participation in activities. This also involves disclosing personal information and any data to PTG Energy Public Company Limited and Max Solution Services Company Limited, including affiliated companies, subsidiaries, partners, allies, and service providers of the aforementioned companies, for marketing purposes, presenting information, sales promotions, offering benefits and promotions, conducting various campaigns, presenting product sales, and analyzing the usage of products or services by members.

In cases where it is necessary to request a copy of the national identification card or official documents used to verify personal identity, the Group understands well that explicit consent must be obtained from the owner of personal data in order to process sensitive personal information. Such sensitive personal information includes, but is not limited to, race, religion, blood type, as well as other sensitive information as defined by law.

Once the Group has obtained clear and explicit consent from the owner of personal data, the Group may collect, use, and disclose sensitive personal information, including facial recognition and fingerprint data, for purposes such as ensuring the safety of individuals and property, including recording work hours, and other relevant purposes.

Using Personal Data for The Original Purposes

The Group has the right to collect, use, and disclose personal information that the Group collected before the effective date of the Personal Data Protection Act, provided that the collection, use, and disclosure of such personal information comply with the original purposes as required by law and the criteria specified in the aforementioned law.

If the owner of personal data does not wish to allow the Group to continue collecting, using, or disclosing such personal data in the future, the owner of personal data can immediately notify the Group to withdraw consent.

Furthermore, the owner of personal data also has the right to exercise the rights of the owner of personal data in various matters as provided by law, by notifying through contact channels,

complaints, or reports of breaches at any time. However, the withdrawal of consent may be subject to limitations under the law or contractual obligations. It should be noted that the withdrawal of consent from the owner of personal data will not affect the processing of personal data provided or performed previously in accordance with the law.

Personal Data Disclosure

The Group will not disclose personal information unless consent is obtained from the data subject or it is necessary to disclose or report personal information to another person as allowed by law without requiring consent or to comply with legal obligations.

Upon obtaining consent from the data subject, the Group may disclose personal information and any data to PTG Energy Company Limited and Max Solution Service Company Limited, including affiliated companies, subsidiaries, joint ventures, partners, allies, and service providers of the aforementioned companies, for marketing purposes, news presentation, sales promotion, benefit and promotion programs, campaign creation, product presentations, and analysis of the usage of products or services by members.

The Group may share personal information with affiliated companies within the Group or with external parties to carry out activities related to auditing accounts, seeking legal advice, pursuing legal cases, and undertaking any other activities necessary for conducting business, as specified in the purposes outlined in this policy.

Data Retention, Duration, and Security Measures

The Group will retain personal data only as necessary to achieve the purposes stated in this policy. The duration of personal data retention will be considered appropriate and in line with contractual periods, legal expiration periods, and the necessity to retain personal data for the periods required by law to establish legal rights or exercise legal claims. In this regard, the Group will retain the data for a period not exceeding 10 years after the termination of the relationship between the data owner and the Group or from the last contact with the Group onwards.

The Group establishes security measures to appropriately safeguard personal data, covering data stored in document format, electronic systems, computer systems, or various tools. These measures adhere to international standards, providing data owners with confidence in the security system for the personal data of the Group. These security measures include protection against loss, unauthorized access, use, alteration, or unauthorized disclosure of personal information or actions without legal authority.

The Group limits access and uses technology to maintain the security of personal data, preventing unauthorized attacks or access to the computer or electronic systems of the Group. Additionally, the Group will act in accordance with the aforementioned guidelines when disclosing personal information to external parties for processing personal data, ensuring that data owners can be confident that the Group will oversee and ensure that such individuals process the data appropriately in compliance with instructions.

Rights as The Owner of Personal Data

Under the Personal Data Protection Act, as the owner of personal data, you have the right,

according to the law, to request access to or copies of personal data collected, used, or disclosed by the Group. You also have the right to request the transfer of data in a format established and readable electronically. Additionally, you can request the Group to send the data to another person as desired (the Group reserves the right to charge fees, to be determined based on actual costs).

As the owner of personal data, you have the right to object to the collection, use, or disclosure of personal data as required by law. You can request the deletion, destruction, or transformation of personal data into non-identifiable information by any means. Moreover, you have the right to suspend the use of personal data, unless there are legal limitations set by the Group that prevent compliance with your request.

Furthermore, if you have given consent to the Group for any purpose, you can withdraw your consent at any time unless such withdrawal is subject to legal or contractual limitations. The withdrawal of consent does not affect the processing of personal data performed or undertaken before the withdrawal in accordance with the law.

The Group will make every effort to collect accurate and up-to-date personal data to ensure completeness and prevent misunderstandings. As the owner of personal data, you have the right to request the correction or modification of personal data if you find that there have been changes or inaccuracies.

The exercise of your rights as the owner of personal data must comply with the law. In this regard, the Group may reject the exercise of your rights according to legal limitations as specified by law.

You, as the owner of personal data, have the right to file a complaint with the Data Protection Officer or the person responsible for overseeing personal data if the Group fails to comply with any legal requirements. To submit a request for the exercise of your rights, you can contact the Data Protection Officer (DPO) or the designated personnel responsible for personal data through the contact channels specified in this policy. The Group will consider and notify the results of the assessment within 30 days from the date of receiving your request.

In case the Group rejects the exercise of your rights, it will provide reasons for the denial simultaneously with the rejection.

Cookies and The Use of Cookies

In the case of visiting the website, the Group may place cookies on the device to automatically collect information about the personal data owner. Some cookies are necessary for the proper functioning of the website, while others are convenience cookies for the website visitors. The personal data owner can find additional information in the cookie policy of the Group at https://www.ptgenergy.co.th/AboutPTG/Cookiepolicy.

Modification of Personal Data Protection Policy

The Group may periodically review, modify, and amend this Personal Data Protection Policy, at least once a year, to align with best practices, regulations, rules, and relevant laws. In the event of any modifications or changes to this Personal Data Protection Policy, the Group will promptly publish the updated policy on its website and other channels. This is to allow data owners to consider and accept it electronically or through other methods. If data owners, in their capacity as users, have taken actions

to accept and approve the updated policy, it will be deemed that the additional and amended policies are part of this existing policy.

Breaches of Personal Data Protection Policy

Failure to adhere to best practices, policies, or personal data protection measures as required by law for employees or staff of the Group may result in misconduct and disciplinary action in accordance with company regulations. For personal data processors, there may be a violation of the personal data processing agreement and may be subject to penalties as specified under the Personal Data Protection Act of 2019, including subsidiary laws, rules, regulations, and relevant orders.

Yours Sincerely,

PTG Energy Group

Announced on March 1, 2021

Revised Edition on December 15, 2023

Contact Details and Whistleblowing:

PTG Energy Public Company Limited

90 CW Building Tower A, 33rd Floor, Ratchadaphisek Road,

Huai Khwang Subdistrict, Huai Khwang District, Bangkok 10310

Phone: 02-168-3377, 02-168-3388

Email: dpo@pt.co.th

Website: www.ptgenergy.co.th