NIPA Technology Co.,Ltd.
72 NT Bangrak Building, 4th floor, Suite 401-402, Charoenkrung Road,
Bangrak, Bangrak, Bangkok 10500, TAX ID 0105539071246
0-2107-8251 0-2639-7770
www.nipa.co.th www.nipa.cloud

# Data Privacy Policy

## 1. Definition

"**The Company**" means NIPA Technology Co., Ltd.

"**The Customer**" means the person or entity that owns the personal data and can access the services of NIPA Technology Co., Ltd.

"**Authorized Person**" means a person who is assigned by the company to have the authority to approve any application in the context of the Company.

"**Executive and Employee**" mean executive, manager, officer, temporary worker, and contract worker of NIPA Technology Co., Ltd.

"**Data Subject**" means a natural person about whom a controller holds personal data and who can be identified, directly or indirectly, by reference to that personal data.

"**Minor**" means a person under the age of 20. Except for a person aged under 20 and legally married, resulting in an adult under the provisions of the law.

"**Incompetent Person**" means a person with a disability, or having a mental disorder, or behaving recklessly, or addicted to alcohol, or any other similar cause until unable to self-manage, or behaving in a way that is detrimental to one's own or family's property. He or she is adjudged by the Court to be incompetent on the ground of the unsound mind, and as such, for the purpose of giving any consent, the consent of the guardian with the power to act on behalf of the incompetent person must first be obtained.

"**Quasi Incompetent Person**" means a person who has a physical or mental infirmity, habitual prodigality (wastefulness) or habitual intoxication, or other similar causes that make him incapable of managing his affairs, or whose management is likely to cause detriment to his property or family, maybe adjudged as quasi incompetent by the Court upon an application by any of the persons specified in Section 28.

"**Curator**" means a person who is assigned by the Court to take care of a quasi-incompetent person. The conduct of which by a quasi-incompetent may detriment to his property or family, the Court is empowered, in giving and order effecting any person to be quasi-incompetent or upon the application made subsequently by the curator, to instruct the quasi-incompetent to obtain the consent of the curator prior to the conduct of such acts.

"**Guardian**" means a person who is entrusted by law and who has the legal right and responsibility of taking care of someone who cannot take care of him or herself, such as an Incompetent person.

"**Personal Data**" means any information relating to a person, which enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased Persons in particular, such as name, surname, email, photo, fingerprint, and identification code. These can identify a person directly or collect location or cookie information, which makes it possible to indirectly identify an individual. Furthermore, when the unidentified data is combined with other information, it creates a new set of data that can identify the personal data and privately save it, such as an address, gender, and age. This combined set of data can be used to identify an individual and becomes personal information. Information may be collected in a variety of ways, either directly (e.g., through a relationship manager, salesperson, or call center) or indirectly from other sources (e.g., social media, third-party online platforms, or other publicly available sources), service providers, business partners, official agencies, or third parties. The type of collected information depends on the customer relationship and the services or products the customer requests.

"**Sensitive Data**" means any personal data about racial or 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 data which may affect the data subject in the same manner as to be prescribed by the PDPC.

"**Biometric Data**" means the personal data arising from the use of technics or technology related to the physical or behavioral dominance of a person, which can be used to identify such person apart from other persons, such as the facial recognition data, iris recognition data, or fingerprint recognition data.

"**Public Data**" means the personal data that the owner has made public, such as a social media profile. When there is a use of information and login codes of social media credentials such as Facebook, Twitter, and Line to connect to or access any of the Company's services such as Social Media Account ID, interests, likes, and friends list of personal data subjects, the owner can control the privacy through the social media account settings that are provided by the service provider.

"**Data Controller**" means a person or a juristic person who has the power and duties to make decisions regarding the collection, use, or disclosure of personal data.

"**Data Processor**" means a person or a juristic person who operates in relation to the collection, use, or disclosure of personal data under the orders given by or on behalf of a data controller.

"**Data Processing**" means any action taken on personal data or personal data sets, either by automatic methods or not, such as archiving, recording, organizing, changing or modifying, receiving, considering, using, disclosing, publishing, or any other action that causes its availability, placement or combination, limiting, deleting, or destroying.

"**Application**" means a program or set of instructions used to control the operation of a mobile computer and its peripherals in order to function as a command and response to a user's requirements. The application must have a User Interface (UI) to act as a connector between the various usages.

"**IP Address**" means the numerical symbols assigned to each device, such as computers or printers, that are involved in a computer network that uses the Internet Protocol to communicate.

"**Cookie**" means small files of the Company's information that a web server generates to collect personal data and sends to a web browser or other devices that are connected to the internet.

"**Office**" means the Office of the Personal Data Protection Committee.

**2. Responsibilities and Liabilities**

2.1 The Board of Directors is responsible for monitoring the protection of personal data by the law and government regulations and appointing or modifying the Personal Data Management Team to support the procedure of the Committee.

2.2 Data Governance is assigned by the Committee to do as follows:

- To supervise the procedure of the Personal Data Management Team.
- To offer guidance and a review of policies, along with an operation for personal data management.
- To suggest recommendations and consider the objectives, policies, proposals, procedures, processes, and documents related to personal data management.
- To monitor and evaluate the performance of personal data management.
- To appoint or modify the Personal Data Management Team to support the Committee's operations as appropriate.
- To be able to invite relevant agencies to attend in order to provide clarification or benefit for the operations.
- To supervise the policy's implementation and have the authority to approve, change, and revise this policy.

2.3 Chief Executive Officer is responsible for managing and controlling operations relating to the collection, use, and disclosure of personal data by the law and regulatory requirements, including providing effective data security.

2.4 Employees are obliged to comply with this policy. Regulations and the Company rules, as well as laws and other relevant rules terms, are strictly enforced.

**3. General Provisions**

3.1 The protection of personal data in this policy covers the personal data of an individual customer.

3.2 The Company requires that the DPO be required to review this policy at least once a year or when there is a significant change in the performance of this policy. Any changes will be announced on the Company's website at www.nipa.cloud.

3.3 The Company collects, uses, or discloses personal information only before or at the moment of obtaining the consent of the personal data subject. Except when the Company makes personal data unidentifiable or legitimately supports it as follows:

- It is crucial to comply with the terms of the contract.
- It is a legal procedure.
- It is crucial under our legitimate rights, without exceeding the extent that the subject of personal data can reasonably be expected.
- It is crucial for carrying out the social mission.
- For preventing life hazards.
- For preparing historical documents or archives for the public benefit.

3.4 The Company collects the personal data only as necessary for legal purposes and informs the data subject of the details of personal data collection, as legally required.

3.5 The company deletes or destroys the personal data or makes it unidentifiable at the expiration of the retention period or beyond the necessity to collect personal data, or as requested by the personal data subject, or upon the withdrawal of consent by the personal data subject unless there is a legitimate cause or an official rule that makes the Company must continue to keep that personal data.

3.6 The Company takes responsibility for personal information securely. This includes consideration of the data subject's privacy and the confidentiality of personal data.

**4. Data Subject's Consent**

4.1 Requesting consent to collect, use, or disclose personal data from the personal data subject must be done explicitly. This can be done in the form of a letter or electronically via an electronic system, except under the condition that consent cannot be obtained by such means. Other ways of acquiring consent must include compelling proof of the data subject's consent.

4.2 The Personal Data Subject must be informed of the purpose for which the personal data is collected, used, or disclosed in a clear, understandable manner, not deceive or mislead the data subject for the purpose, and take the data subject's independence into account for the consent of personal data.

4.3 In the case where data subject is a minor who is not of legal age by marriage or has no status as a person who has reached the age of majority, it is necessary to obtain consent from the person who has parental power to act on behalf of the minor.

4.4 In the case that the data subject is an incompetent person, it is necessary to obtain consent from the guardian who has the authority to act on behalf of the incompetent person.

4.5 In the case that the data subject is a quasi-incompetent person, it is necessary to obtain consent from a curator who has the power to act on behalf of the quasi-incompetent person.

4.6 In the case of the data subject or the person authorized under Articles 4.3, 4.4, and 4.5, wanting to withdraw the consent previously given, the subject has to follow the process as easily as giving consent. If the withdrawal of consent affects the subject of personal data in any matter, inform them of the consequences.

4.7 The company must collect, use, or disclose personal data only for the purposes for which it was informed by the data subject. It cannot be done unless the subject of the personal data has been informed of the new purpose of the personal data and has given consent before it is collected, used, or disclosed.

**5. Objective of collecting personal data**

5.1 Personal data must be collected to use it in the Company's operations in various fields, as required by law or government regulations.

5.2 Before or during the collection of personal data, please provide the following information to the owner:

- The purpose of collection is to allow for the use or disclosure of personal data.
- The necessity for data subjects to submit personal data in order to comply with the law or enter into a contract, as well as the consequences of failing to do so.
- Personal data that will be collected and for how long.
- Persons or entities to whom personal data may be disclosed, including a list of such persons or entities (case-by-case).
- Personal data rights by law.
- Information about the company and data protection, as well as contact details and methods.

5.3 The personal data collected must be accurate and complete in accordance with the facts informed by the personal data subject. If the information has changed, make corrections to be accurate and up-to-date.

5.4 Collection of sensitive personal data requires the consent of the data subject unless there is a legitimate basis for it by having to seek approval from the authorized person.

5.5 Collection of personal data from sources other than those directly from the personal data subject must be notified within 30 days from the collection day by obtaining the consent of the data subject unless there is a legitimate basis for it by having to seek approval from the authorized person.

5.6 Personal data collection must be documented to collect each type of personal data along with information about the Data Controller Officer, data retention, rights, and other access methods to personal data, and conditions concerning persons entitled to access to personal data, including other details as required by law for the data subject or the office to inspect.

**6. Personal Data Use and Access**

6.1 The Company's employees can access or use personal information as needed for work and in compliance with the Company's rights. Permission from the authorized person is required if the employees need to access restricted personal data.

6.2 The Company's employees have to use personal data for the purposes for which it was collected or only with the consent of the data subject unless there is a legitimate basis to support it.

6.3 The Data Controller and Data Processor must allow the Company's authorized employees to access personal data.

**7. Acquisition**

The Company collects personal data through the following processes:

7.1 Personal data is obtained directly from the data subject.

7.2 Personal data from third parties such as agents, merchants, or companies providing data collection services, partners, etc.

7.3 Personal data is obtained by visiting the website, such as the name of the Internet service provider and IP address through internet access, the date and time of visiting the website's pages, and the address of the website which is directly linked to the Company's website.

7.4 Personal data is obtained from public records and non-public records that the Company is legally entitled to collect.

7.5 Personal data is obtained from government agencies and regulatory authorities that exercise legal powers.

8. Personal Data Collection and Disclosure

8.1 Disclosure of personal data to third parties or organizations outside the Company requires consent from the data subject and must be approved by the Data Governance Council unless it is in compliance with laws or official regulations.

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

8.1.1 A person who is authorized to act as an intermediary includes transportation companies, storage companies, and information development companies that use the system to carry out the Company's various activities.

8.1.2 Partners, business partners, and/or external service providers provide services in offering benefits and other services to the data subject, including the development and improvement of the Company's products or services such as data analysis, data processing, IT services, and related infrastructure, customer service platform development, email and SMS sending, website and mobile application improvement, satisfaction surveys, and research, customer relationship management with credential data. In the case of a juristic person, the personal data protection standard is required.

8.1.3 A government agency, a government, or another legal entity to comply with the law, order, request, or coordinate with various departments on a related legal matter.

8.2 The action of receiving personal data from individuals or organizations outside the Company must ensure that the received personal data is supported on a legitimate basis and must be approved by Data Governance Council unless it is in compliance with laws or official regulations.

The Company will collect data that the data subject has directly given to the company or personal data that the Company receives from the service or the Company's operations through all channels, which include the following channels:

8.2.1 Personal data is obtained when the data subject registers or fills out an application form requesting to participate in various activities of the Company or use the Company's services, such as name, surname, ID number, phone number, date of birth, address, email, etc.

8.2.2 Data derived from subscriptions or activity participation, data on creating an account that creates a profile that contains details of personal data provided to the Company for accessing the service Company's channels, like the Company's website, for example, web application accounts services of the

Company, as well as personal data provided for various applications, such as applying to participate in activities and/or contacting the Company via the website or through other channels as specified by the company.

8.2.3 Subscription data from the survey or information about participating in activities such as satisfaction, interest, consumer behavior, etc.

8.2.4 Data about transactions with the Company or others, such as information about applying to be a representative, bidding data, including bank account number, or information about the transactions depends on the type of transaction of the data subject.

8.2.5 Data from the Company's website, other sites, or the company's application or operated by the Company, social media usage, and interaction with the Company's online advertisements, the version and type of computer program used to open the website, the type of device used to access the service, such as a personal computer, laptop, or smartphone, operating system and platform information, IP address of the device, or terminal device, location data, and information about the services and products of the data subject's visit or search.

8.2.6 Data from the contact record of the data subject with the Company, which is stored in the form of messages of service recipients, satisfaction evaluations, research and statistics, conversation recordings, CCTV recordings, when the data subject contacts the company, such as the company's customer service, including research media information, such as SMS, Social Media, applications, or emails, etc.

8.2.7 Social media profile data. When using social media credentials such as Facebook, Twitter, and Line to connect or access the Company's services, such as Social Media Account IDs, Interests, Likes, and friends list of data subjects, which can control the storage privacy through the social media account settings provided by the social media service provider.

8.3 In the case that the Company lets a person or organization outside the Company collect, use, or disclose personal data on behalf of the company, this must be done by a personal data processor who has appropriate security levels and is equivalent to the Company's standards in accordance with the security policy of the external IT service providers' management. Moreover, there must be an agreement between them to control the processing of the personal data processor in accordance with the law by clearly stipulating the purpose or order for the collection, use, or disclosure of personal data to the personal data processor and setting measures to prevent personal data processors from collecting, using, or disclosing personal data received from the Company without the Company's permission.

9. **Sending or Transferring Personal Information Overseas**

In the case that the Company transfers and/or sends information to foreign countries, the Company has to set standards for the agreements and/or contracts with business entities. Personal data protection and compliance with applicable laws to ensure that personal data is safely protected, such as

9.1 In the case that the company needs to store and/or transfer personal data into a database.

9.2 In cloud computing, the Company will consider organizations with international security standards and will collect personal data in an encrypted format or other methods that cannot identify the data subject, etc.

In addition, the data subject can check the list of third parties to whom the Company will disclose personal data from www.nipa.cloud. The list of the Company's third parties that will disclose the data subject's information might increase or decrease, which the Company will keep the data up to date.

10. Security and Confidentiality

In order for the data subject to have faith in the company's security and confidential management, the Company adheres to the Information Security Policy, as well as complies with international standards and business continuity management, in accordance with the law.

The company has put in place safeguards to protect the data subject by restricting access to the data subject's information. The data will be accessible by the designated person who needs to utilize such personal data in presenting the Company's products and services, such as the Company's employee, who has been granted access to that personal data by the Company. The employee must adhere to and strictly comply with the Company's personal data protection standards as well as maintain the confidentiality of such personal data. The Company has implemented both physical and electronic protections in accordance with applicable regulatory standards.

When the Company makes a contract or agreement with a third party, the Company will determine the security measures for personal data confidentiality in order to ensure that the personal data it holds is secure.

11. **Records of Processing Activities (RDPR)**

The Company has to store and record an inventory of the data processing in order to comply with Article 39 of the Personal Data Protection Act. The record of the data inventory has to be kept in both cases of the Company's personal data controller and the case where the company is acting to process personal data on behalf of another personal data controller to comply with the law.

The record of personal data processing activities includes at least the following items: types of data subjects, personal data types and specifics that are collected or used for legal purposes in the data processing period, period of retention, disclosure of personal data, and a description of the security standards that the Company has in place. Records of personal data processing activities must be accurate, complete, and up-to-date.

12. **Data Subject Rights**

Data Subject has the following rights:

- The right to request recognition of the existence of personal data characteristics as well as the purpose of the Company's use of personal data.
- The right to access and request a copy of their personal data, for which the company will have an appropriate procedure for you to first confirm your identity with the Company.
- The right to request that their personal data be modified or changed so that it is accurate, current, and complete, and does not cause misunderstandings.
- The right to object to the collection, use, or disclosure of personally identifiable information, as well as the right to object to personal data processing.
- The right to request a suspension of use or the temporary disclosure of personal data.
- The right to request, delete, or destroy personal data, or to have personal data rendered unidentifiable to the person who owns the data.
- The right to inquire about the collection of personally identifiable information when the customer has not consented to the collection or storage of such information.
- The right to revoke previously granted consent to the collection, use, or disclosure of personal data by the company. Withdrawal of consent does not affect the collection, use, or disclosure of personal data of the data subject who has given consent.

In this regard, the Company has established a communication channel through which you can exercise your rights as outlined in Article 20, and the Company will proceed and consider your request within 30 days from the date of receipt of the request. However, the company might decline to operate in accordance with the data subject's rights as required by law or according to the contract made with the company if the data subject loses benefits. In this regard, the Company has established a communication channel through which you can exercise your rights as outlined in Article 20, and the Company will proceed and consider your request within 30 days from the date of receipt of the request. However, the company might decline to operate in accordance with

the data subject's rights as required by law or according to the contract made with the company if the data subject loses benefits.

Furthermore, deleting, destroying, or putting your personal data in an unidentifiable form or the cancellation of the data subject's consent can only be done under the provisions of the law and the contract with the Company. However, the exercise of such rights may affect the performance of the contract with the Company or other services because the identity of the data subject cannot be identified. Consequently, there may be limitations in the provision of some services that require personal data and may cause the data subject to not gain the benefits of the service and further news from the Company.

13. **Data privacy by design and by default**

The Company must provide proactive and protective measures to protect the privacy of data subjects, starting from the personal data protection risk assessment as part of the system design and development in the infrastructure of information systems, including changes affecting the processing of personal data.

To ensure that the protection of the appendix's personal data is an essential component of all technological and business activities, personal data protection measures must be implemented as the standard requirement.

14. **Privacy Incident Management**

The company has set working standards in order to efficiently and timely manage any abnormal situations which could impact personal data the company is taking care of. The standards are in accordance with the situation responding procedures, which affect personal data security or personal data breach management procedure.

15. **Personal Data Collecting Duration and Locations**

The company will collect personal data as long as it is necessary, considering the objectives and needs the company has to collect and process. The compliance with requirements of applicable law is included. The company will collect personal data until the data subject and the company will not interact after a period of time, in accordance with the terms and conditions of the relevant laws. The data will be collected in suitable locations according to the type of personal data. However, the company might need to continually collect the data even after the statutory limitation period has expired, such as during the legal proceedings.

16. **Use of Personal Data for Marketing Purposes**

In addition to the above-mentioned and under-the-provision-of-the-law purposes, the company will use the personal data for any marketing purposes, e.g. delivering promotional documents via mail, e-mail, and any

other means, and direct marketing executions, in order to increase the benefits the data subject will receive from being the company's customer through recommendation of related products and services.

17. **Cookies**

The company will use cookies for collecting the use of data subjects to collect data and statistics, research, analyze trends, as well as improve and manage operation of the website and/or application. Nevertheless, cookie collection is unable to identify the data subject.

18. **External Website Connection**

The company's website will be linked to the third-party websites which might have different privacy policies from the Company's. The data subject should read the privacy policy of that website to understand the details of the personal data protection, and to make a decision on the disclosure of personal data. The company will not be responsible for any contents, policies, damages, or actions caused by the third-party website.

19. **Personal Data Protection Officer**

The company has appointed a Personal Data Protection Officer to monitor the personal data collection, use, or disclosure. The executions should comply with the Personal Data Protection Act B.E. 2562 (2019) and the company's policies, regulations, announcements, and orders. The officer will also coordinate and cooperate with the Personal Data Protection Office.

20. **Privacy Policy Questions**

If you have any questions or concerns about this Privacy Statement or your data's protecting management, you can contact us.

21. **Contacts**

If you have any concerns about the company's privacy policy, the data collected by the company, or you would like to exercise any of the PDPA following section 12., you can contact to:

Company Name NIPA Technology Co., Ltd.

**Address** 72 NT Bangrak Building, 4th Floor, Suite 401-402, Charoenkrung Road, Bangrak, Bangrak, Bangkok, 10500

**Website** www.nipa.cloud

**Call center** 02 107 8251 ext. 444

**Email** dpo@nipa.cloud

22. **Contact Appropriate Authority**

If you would like to report a complaint or feel that the company responds your concerns unsatisfactorily, you can contact and/or complain to the Personal Data Protection Commission Office from the information below:

Personal Data Protection Commission Office

Office of the Permanent Secretary, Ministry of Digital Economy and Society

Email pdpc@mdes.go.th

Tel. 0-2142-1033