Puumsoft Company Limited ("Puumsoft", "we" or "us") would like Vendor ("you") do understand this Privacy Policy. This Privacy Policy describes how we handle your Personal Data and Sensitive Data, including collection, storage, use, disclosure and your rights relating to your Personal Data and Sensitive Data.

1. What is Personal Data?

Personal Data is any other data which identify yourself (no matter it can be identified by itself, or together with other information)

Vendor is the person that contacts the customer to coordinate with and provide assistance to Puumsoft.

2. Personal or Sensitive Data Processing

2.1 We needs to correctly, completely, sufficiently receive your personal information in order to perform the obligations under Contract, with the following data:

- Name and surname
- Telephone number
- E-Mail

Below are details of our processing activities:

Processing Area	Activities	Basis for Processing
Coordination/Use of Service	For use in coordinating the project and use of services.	Contract/Before contract

2.2 We will strictly and properly implement the Personal Data security measure and be compliant with Privacy Policy in order to protect your Personal Data or Sensitive Data from any loss, destroying, modifying, accessing or disclosing without permission or legality in accordance with Data Security Policy and Procedure and IT Security Guideline and Policy.

2.3 If there is any change and/or adding of the purpose of processing e.g. processing based on contract or lawful basis etc., we will inform you of new purpose via Puumsoft website, poster announcement or e-mail. We will record such changes for evidence. In addition, we may request your consent before processing any activities of new purposes (if consent required by law).

3. We process your Personal Data restrictively

3.1 We will restrictively process your Personal Data or Sensitive Data by using legitimate and fair method and within the scope of the specified objective.

3.2 Other than the specified objective, we will obtain your consent prior to processing Personal Data; unless

> (1) It is required by laws;
>
> (2) It is beneficial to you, given that it is impossible to obtain your consent at that time;
>
> (3) It is beneficial to your or someone else's life, health or security;
>
> (4) It is for a purpose of investigation of an officer or judicial process of court;
>
> (5) It is beneficial to research or statistics preparation.

3.3 In case of necessity, we may collect your Sensitive Data, obtained from outside sources only as necessary and will notify the data owner within 30 days or will seek permission from the customer (in the case the law requires it), all for the purposes above and to bring customer's data up-to-date, improve quality and efficiency for the company.

4. Transfer to Third Country

We may transfer customer personal data to a foreign country to support operations of the company. The customer grants permission to the company to transfer customer personal data to a foreign country to persons or companies in another country, or into another country's jurisdiction, even if personal data protection laws in such a country may be at the same or less than the level of protection in Thailand. In any case, the company will follow suitable steps in protecting the customer's personal data at the same protection level as in Thailand.

5. Your participation as Personal Data owner

The customer has a right to check the existence of personal data, type of data and the purpose of the use of the data. In addition, the customer has a right to:

5.1   Request a copy of the personal data in electronic form that can be transferred outside of the company or the customer can request direct transfer of the data from the company.

5.2 Request the company to modify, update or correct the personal data to avoid any misunderstanding.

5.3 Dispute or prohibit the use or revealing of customer personal data for purposes of marketing or other purposes.

5.4 Request the deletion of customer personal data when there is no useful purpose for the data, including limiting the use of the data in the case the data cannot be deleted.

5.5 Reveal the source of where the personal or sensitive data was obtained in the case the customer did not grant permission to obtain or store such personal data.

5.6 Cancel any permission granted to obtain or use the personal data.

5.7 Request the transfer of the personal data to other data protection officers.

5.8 Lodge a complaint with the relevant organizations in the case the customer suspects there has been a breach of personal data.

However, the customer's rights must be in compliance of the Personal Data Protection Act as well as the Privacy Policy and other relevant data regulation of the company.

Remark:

If the company processes your Personal Data and/or Sensitive Data based on Contract, legitimate interest or legal obligation basis, we reserve our right to refuse your right in (5.4).

Please note that if the customer chooses to exercise your right in (5.4), the company may not be able to perform the obligations under the contract which might result in contract termination and/or the inability to provide the benefits under the contact to you.

If the customer refuses to provide crucial data that the company may not be able to perform the obligations under the contract which might result in contract termination and/or the inability to provide the benefits under the contract to you.

6. Data Retention Period

We reserve our right to process and disclose your Personal Data and your Sensitive Data and any relevant authorities as required by laws, whichever the case may be, within 2 years from the job application date (for Candidate) and 10 years from the last working date (for Employee).

7. Limitation of liability

Although the company employs the strictest measures and best technology to protect personal data security, the company is not able to guarantee zero incidents of personal data security breach. Therefore, the company reserves the right to not be held responsible for any loss or damages to personal data in all cases.

8. Notification of personal data security breaches

Employees may notify any breaches of personal data to the Data Protection Officer (DPO) of the company as specified in section 9 of this policy for the benefit of the employee. The company requests that the employee notify the company of such breaches as soon as possible after the employee discovers the breach.

9. Changes to this Privacy Notice

The customer may ask questions regarding this Privacy Policy or the methods in obtaining, storing, revealing or making use of personal data and how to exercise their right under the law with the Data Protection Offficer at:

- Email: dpo@puumsoft.co.th

- Website: https://www.puumsoft.co.th

- Telephone: 02 260 0100-2

- Address: 54 BB Building 14th Floor Room 1402, Sukhumvit 21 Road, Klongtoeyneau, Wattana, Bangkok 10110.

10. Changes to the Personal Data Protection Policy

The company may make improvements or modifications to this Personal Data Protection Policy from time to time to comply with your company's policy, operations, or suggestions and or recommendations from your company. The company will announce the changes officially before actually making any changes. Your company may notify you directly through your company's communication channels such as bulletin boards or e-mail.

This policy is effective from 7 October 2022.

Arporna Paul Sribhibhadh

Managing Director