THAI PRIVACY LAW - FREQUENTLY ASKED QUESTIONS
July 2024

This document is provided for informational purposes. It is not intended to provide legal advice. Salesforce urges its customers to consult with their own legal counsel to familiarize themselves with the requirements that govern their specific situations. This information is provided as of the date of document publication, and may not account for changes after the date of publication. For further information on our privacy practices, please see other resources on the Privacy website available here.

At Salesforce, Trust is our #1 value. Nothing is more important than the success of our Customers and the protection of our Customers' data.

We know you may have questions about how Salesforce's online services support your organization's compliance with Thailand's Personal Data Protection Act B.E. 2562 (2019) ("PDPA"). To help you develop a better understanding, we have created this FAQ to answer some of the most common questions we are asked.

1. The Personal Data Protection Act

a. What is the Personal Data Protection Act?

The Personal Data Protection Act B.E. 2562 (2019) ("PDPA") is the first national law to comprehensively address privacy and data protection in Thailand. The PDPA took effect in June 2022 and applies to the collection, use or disclosure of personal data by a data controller or a data processor.

b. Does the PDPA affect my organization?

The PDPA applies to the collection, use or disclosure of personal data by organisations that are in Thailand, regardless of whether the collection, use or disclosure of personal data takes place in Thailand or not.

The PDPA has an extraterritorial scope that expands Thailand's data protection obligations to cover all personal data processing activities relating to Thailand-based data subjects,

similar to the GDPR. The PDPA applies to data controllers and data processors that are outside of Thailand where the collection, use or disclosure of personal data is of data subjects who are in Thailand, provided that (i) the controller or processor's activities relate to the offering of goods or services to data subjects in Thailand, regardless of whether payment is required and/or (ii) the data subject's behavior in Thailand is being monitored.

c. What does Salesforce think about the PDPA?

Salesforce recognizes privacy as a fundamental human right and business imperative. To protect people, promote trust in technology, drive innovation, and support the global digital economy, we welcome laws like the PDPA. Salesforce is also dedicated to helping our Customers comply with their obligations under the PDPA when using our services. Salesforce's current Data Processing Addendum ("DPA") is tailored to meet global data protection laws and regulations requirements, including those under the PDPA. We will continue to monitor the PDPA regulations and, to the extent necessary, make modifications to help enable compliance.

d. Do Salesforce customers need a new DPA?

Under the PDPA, Customers are likely required to enter into a DPA with Salesforce to ensure that the activities carried out by Salesforce are in accordance with a data processor's obligations under the PDPA. Customers who signed earlier (pre-2022) versions of our DPA, or who entered into a Master Subscription Agreement without a DPA, can sign our current DPA at any time (see Salesforce's DPA FAQs for more information).

e. Can Personal Data be transferred out of Thailand?

Under the PDPA, Personal Data can be transferred out of Thailand, including to foreign countries or international organizations provided that (i) the destination countries or international organizations have an adequate level of protection as prescribed by the PDPC (similar to an adequacy decision under the EU GDPR), (ii) the international transfer is to an organization within the same group/affiliated business, for joint business operations and the data controller or the data processor has an internal policy with safeguards for cross-border transfer of personal data (similar to the GDPR's binding corporate rules) or (iii) the controller or processor provides suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedies according to the rules and methods as prescribed by the PDPC (i.e., as set forth in the Salesforce DPA).

f. Is Salesforce able to comply with the Notifications for the Protection of Personal Data Transferred to a Foreign Country?

In March 2024, new regulations were prescribed by the PDPC regarding offshore transfers of Personal Data. Those regulations set out two options for offshore transfers: contractual terms aligning with published criteria, and contractual terms aligning with another global model contract, such as the GDPR SCCs or the ASEAN Model Clauses.

We believe Salesforce's current DPA, tailored to meet global data protection laws and requirements, is sufficient to meet the published criteria for contractual terms, set out in the March 2024 regulations. In addition, we make available the GDPR SCCs to all our Customers as part of our DPA.

2. Data processing by Salesforce

a. What laws and regulations are applicable to the processing of personal data by Salesforce and its Customers?

The definition of Data Protection Laws and Regulations in our DPA means "all laws and regulations [...] applicable to the Processing of Personal Data" under the DPA, and which includes the PDPA. While certain jurisdictions are specifically called out in the definition, regulations of those jurisdictions are only relevant to the extent that they relate to the Processing of Customer Data and Personal Data.

b. What are Salesforce's and the Customer's roles in processing personal data?

To align with terminology used in many global data protection laws and regulations, including the PDPA, Salesforce acts as the "processor" with respect to personal data submitted by Customers to Salesforce's services. Customers either act as a "controller" or a "processor" of such personal data.

It is for the Customer to determine whether it is acting as a controller or a processor in uploading personal data to Salesforce's services. In both scenarios, Salesforce acts as a processor and processes such personal data only in accordance with the Customer's documented instructions.

3. Data Subject Requests

How does Salesforce handle requests from data subjects?

If Salesforce receives a data subject request from a Customer's customer or end user, Salesforce will, to the extent legally permitted, ask the data subject to contact the relevant Customer directly about the request. Salesforce will also, in accordance with its commitments made to Customers, promptly notify the Customer, although we will not further respond to the data subject request without a Customer's prior consent.

Salesforce assists its Customers by offering appropriate technical and organizational measures, insofar as this is possible, to enable its Customers to fulfill their obligation to respond to data subject requests.

4. Sub-processors

a. Does Salesforce use sub-processors?

An effective and efficient performance of Salesforce's services requires the use of sub-processors. These sub-processors can include affiliates of Salesforce as well as third

party organizations. Salesforce's use of sub-processors may require the transfer of Customer Data to sub-processors for purposes like hosting Customer data, providing Customer support, and ensuring the Salesforce services are working properly. Salesforce takes responsibility for the actions of its sub-processors.

Up-to-date information about the hosting locations for each Salesforce service and the identities and the locations of sub-processors can be found in the applicable Infrastructure and Sub-processor Documentation (available here).

b. How does Salesforce notify its Customers of new sub-processors?

Customers may subscribe to notifications of new sub-processors for each Salesforce service (see here). Salesforce will notify all subscribed Customers of a new sub-processor before authorizing the new sub-processor to process Customer Data. Customers may object to the intended use of a new sub-processor using the procedure set out in the Global DPA.

5. Technical and Organizational Measures

What security measures are in place to protect Customer Data?

Under the PDPA, data controllers are required to have appropriate security measures which meet the minimum standard as specified and published by the Personal Data Protection Committee ("PDPC") to protect personal data against unauthorized or unlawful loss, access, use, alteration, correction, or disclosure.

Salesforce maintains appropriate technical and organizational measures to protect Customer Data, as set forth in the applicable SPARC Documentation (available here).

Please also see Salesforce's dedicated Security page and our Compliance website detailing our compliance certifications and attestations.

6. Security Breach Notification

How would Salesforce notify its Customers in the event of a security breach?

Salesforce maintains security incident management policies and procedures, which are described in the applicable SPARC Documentation (available here). Salesforce commits to notify Customers without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data processed by Salesforce or its sub-processors.

If a Customer is impacted by a security breach, the Customer's Security Contact(s) will be notified. This supports Customers with their obligations under the PDPA to report data breaches to the PDPC without undue delay and to determine whether any mandatory notification obligations to data subjects are triggered. Steps on how to create and maintain your Security Contact List are available here.

7. Government Access Requests

What happens if Salesforce receives a government access request in respect of Customer Data?

At Salesforce, trust is our #1 value. The protection of our Customers' data is paramount, and we safeguard that data with a robust, comprehensive, and transparent privacy and security program. Our privacy and security program is designed to protect Customer Data against unauthorized or unlawful loss, access, or disclosure.

Salesforce is not the owner of Customer Data and, accordingly, if we receive a government request for Customer Data, if permitted by law, we refer the request to the affected Customer so that the Customer can work with the governmental agency directly to respond. We do not disclose Customer Data to government agencies unless compelled by law and we also challenge unlawful requests.

It is rare for Salesforce to receive government requests for Customer Data. Due to the nature of our business, Salesforce generally does not process Customer Data that is of particular interest to law enforcement or intelligence services. A copy of our Transparency Reports detailing the number of government access requests we receive is detailed here.

8. Return and Deletion of Customer Data

What happens to Customer Data after termination or expiration of an agreement with Salesforce?

After termination or expiration of the agreement, Salesforce will return and delete all Customer Data in accordance with applicable laws and the procedures and timeframes specified in the applicable SPARC Documentation (available here). Until Customer Data is deleted or returned, Salesforce will continue to comply with its legal obligations to Customers.

9. Where can I find additional legal documentation and information about Salesforce's services?

- Salesforce's global DPA can be found here.
- Salesforce's global MSA can be found here.
- The Security Privacy and Architecture Documentation (**"**SPARC") detailing Salesforce's security measures, and the Infrastructure and Sub-processor Documentation listing Salesforce's sub-processors, are available on the Trust and Compliance website here.
- Salesforce's Privacy website can be found here, and provides further information on Salesforce's Privacy programme as well as helpful references including white papers on key topics and documents providing information to assist customers with the completion of data protection impact assessments ("DPIAs").

- The Salesforce Compliance website detailing our compliance certifications and attestations can be found here.
- Salesforce also has a dedicated Security page which details best practices, training and security advisories.