

HUAWEI CLOUD Compliance with Thailand PDPA

Issue	2.2
Date	2024-08-05



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

Contents

1 Overview 1

1.1 Scope of Application 1

1.2 Purpose of Publication 1

1.3 Basic Definitions 1

2 Privacy Protection Responsibilities 3

3 Thailand's Personal Data Protection Act (PDPA) Overview 5

3.1 Thailand's PDPA Background 5

3.2 Roles and Basic Obligations 5

3.3 HUAWEI CLOUD's Role under the PDPA 6

4 How HUAWEI CLOUD is Satisfying the Requirements of Thailand's PDPA 8

4.1 HUAWEI CLOUD Privacy Commitment 8

4.2 HUAWEI CLOUD Basic Privacy Protection Principles 8

4.3 Basic Regulation Principles and HUAWEI CLOUD Related Practices 9

5 How HUAWEI CLOUD Supports Customers to Comply with Thailand's PDPA 16

5.1 Customers' Privacy Protection Responsibilities and Obligations 16

5.2 How HUAWEI CLOUD Products and Services Help Customers Implementing Content Data Privacy and Security 19

6 HUAWEI CLOUD Privacy Protection Related Certifications 24

7 Conclusion 26

8 Version History 27

1 Overview

1.1 Scope of Application

The information provided in this document applies to HUAWEI CLOUD and all its products and services available in Thailand.

1.2 Purpose of Publication

This document is intended to help customers understand:

- HUAWEI CLOUD's privacy protection responsibility model;
- Thailand's privacy laws and regulations;
- HUAWEI CLOUD's responsibilities on compliance with Thailand's privacy laws and regulations;
- HUAWEI CLOUD's controls and achievements in privacy management;
- Customers' responsibilities and obligations when falling under Thailand's privacy regulations jurisdiction, as specified in the responsibility model;
- How to leverage HUAWEI CLOUD's security products and services to achieve privacy compliance.

1.3 Basic Definitions

- **Personal Data**
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.
- **Data Subject**
An identified or identifiable natural person.
- **Data Controller**
A natural person or a legal person having the power and duties to make decisions regarding the collection, use, or disclosure of the personal data.
- **Data Processor**

A natural person or a legal person who operates in relation to the collection, use, or disclosure of the personal data pursuant to the instructions given by or on behalf of a data controller, whereby such natural person or juristic person is not the data controller.

- **HUAWEI CLOUD**

HUAWEI CLOUD is the cloud service brand of the HUAWEI marquee, committed to providing stable, secure, reliable, and sustainable cloud services.

- **Customer**

Registered users having a business relationship with HUAWEI CLOUD.

- **Third Party**

A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

- **Account Information**

Personal data, such as names, phone numbers, email addresses, bank accounts and billing information provided by customers to HUAWEI CLOUD when creating or managing their HUAWEI CLOUD accounts. HUAWEI CLOUD acts as the data controller of any personal data included within account information.

- **Content Data**

Data stored or processed during the use of HUAWEI CLOUD services, including but not limited to documents, software, images, and audio and video files.

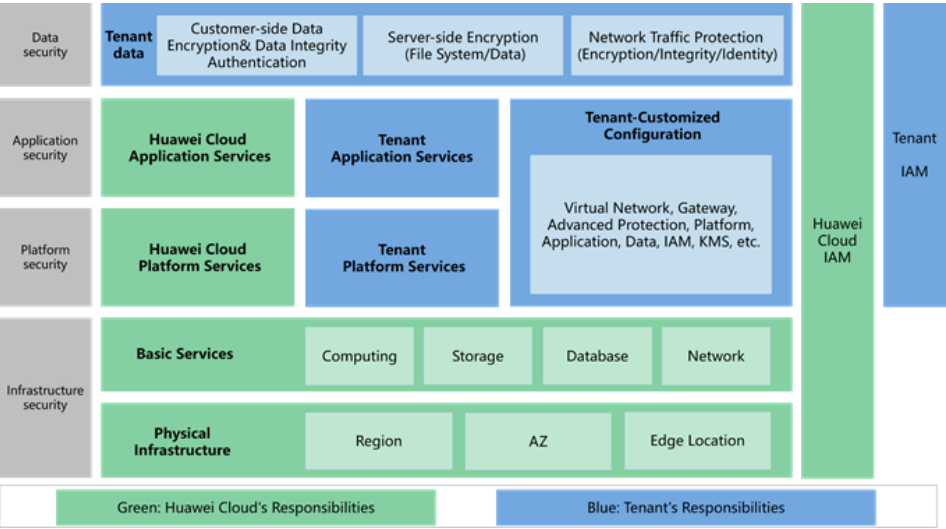
- **Processing**

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

2 Privacy Protection Responsibilities

Due to the complex cloud service business model, the security protection of personal data is not the sole responsibility of one single party, but requires the joint efforts of both the tenant and HUAWEI CLOUD. As a result, HUAWEI CLOUD proposes a responsibility sharing model to help tenants to understand the privacy protection responsibility scope for both parties and ensure the coverage of all areas of privacy protection. Below is an overview of the responsibilities distribution model between the tenant and HUAWEI CLOUD:

Figure 2-1 Responsibility Sharing Model



As shown in the above figure, the privacy protection responsibilities are distributed between HUAWEI CLOUD and tenants as below:

HUAWEI CLOUD: As the Cloud Service Provider (CSP), HUAWEI CLOUD is not only responsible for the security and compliance of personal data collected or processed during business operations, but also for the **platform security** defined by the security and compliance of HUAWEI CLOUD's infrastructure, including the cloud platform and software applications offered to tenants.

- **Protection of Tenant Privacy:** HUAWEI CLOUD identifies and protects tenants' personal data. HUAWEI CLOUD's policy, processes and operations not only resulted in the formulation of privacy protection policies but also in the deployment of active

privacy control measures, such as anonymization, data encryption, system and platform security protections, all helping to ensure the security of tenants' personal data.

- **Platform and Tenant Security Support:** HUAWEI CLOUD is responsible for the security and compliance of the platform and infrastructure included in the cloud service, ensuring the platform and applications' security levels comply with the requirements of applicable privacy protection laws and regulations. At the same time, HUAWEI CLOUD provides tenants with a variety of privacy protection technologies and services in order to help tenants protect their privacy, such as access control, authentication, data encryption, logging and auditing functions, in order to help tenants protect their privacy according to their commercial requirements.

Tenant: As purchaser of HUAWEI CLOUD's products and services, tenants are free to decide on how to use them to store or process content data, which may include personal data. Therefore, tenants are responsible of **Content Security**, which is defined as the security and compliance of content data.

- **Content Data Protection:** Tenants should correctly and comprehensively identify personal data in the cloud, formulate policies to protect data security and privacy, and finally select appropriate privacy protection measures. Specific measures shall include security configuration based on business and privacy protection requirements, such as operating system configuration, network settings, security protection, database encryption, policy configuration and set appropriate access controls and password policies.
- **Respond to data subject requests:** Tenants shall guarantee the rights of data subjects and respond to their requests in a timely manner. In the case of a personal data breach, the tenant shall notify both regulatory authorities and data subjects, and take adequate actions in accordance with regulatory requirements.

3

Thailand's Personal Data Protection Act (PDPA) Overview

3.1 Thailand's PDPA Background

The Thailand Personal Data Protection Act B.E. 2562 (PDPA) came into force on June 1st, 2022. The PDPA regulates the collection, protection, use, disclosure, transfer and other processing operations on personal data.

3.2 Roles and Basic Obligations

The PDPA defines the roles of the data controller and data processor as well as their obligations.

- **The data controller** has the following fundamental obligations:
 - **Obtain Data Subject's Consent:** Personal Data can only be collected after informing the data subjects the purpose of collection and obtaining the consent of the data subjects (unless exceptional circumstances apply). Personal data can only be transmitted to a country or international organization outside of Thailand that does not have adequate data protection standards provided that the data subject has been appropriately informed and his consent was obtained, except in the circumstances mentioned in the PDPA allowing cross-border transfer.
 - **Secure Data Processing:** Deploying appropriate security measures for preventing the unauthorized or unlawful loss, access, use, alteration, correction or disclosure of personal data, and such measures must be reviewed when necessary, or in the event of a change in the technology.
 - **Respond to Data Subject's Requests:** The PDPA gives the data subject the rights to withdraw their consent and to delete, restrict the usage, correct or obtain a copy of their personal data. When the data subject exercises any of his rights, the data controller shall respond within a limited time as stipulated by law.
 - **Record Processing Activities:** Maintaining records of personal data processing activities.
 - **Prevent Unauthorized Use or Disclosure of Personal Data to Third Parties:** Personal data should only be used or disclosed for purposes for which the data subject has given his consent, unless otherwise permitted by the PDPA where a consent is not required. A personal data processing agreement with the data

- processor shall be signed to ensure compliance with the obligations provided in the PDPA.
- **Data Erasure:** Arranging the erasure or destruction of personal data, which has become unnecessary, reaches the end of the retention period, or at the request of the data subject.
 - **Data Breach Notification:** Notifying the Personal Data Protection Committee or the data subject in case of any violation related to personal data according to the rules and procedures set forth by the PDPA.
 - **Appoint a DPO:** Appointing a personal data protection officer.
 - **Appoint a Representative:** If the data controller is not located in Thailand, a local representative of the data controller shall be designated in writing. The representative must be in Thailand and be authorized to act on behalf of the data controller without any limitation of liability regarding the collection, use or disclosure of personal data according to the purposes set by the data controller.
- **The data processor** has the following obligations:
 - **Follow Instructions:** Performing activities related to the collection, use or disclosure of personal data according to the instructions provided by the data controller.
 - **Proof of Compliance:** Complying with the personal data processing agreement signed with the data controller.
 - **Secure Data Processing:** Deploying appropriate security measures to prevent loss or unauthorized access, use, modification and disclosure of data.
 - **Data breach notification:** Notifying the data controller of any violation personal data breaches that occurred, as required in the PDPA.
 - **Appoint a DPO:** Appointing a personal data protection officer.
 - **Record Processing Activities:** Preparing and maintaining records of personal data processing activities in accordance with the requirements and procedures prescribed by the Personal Data Protection Committee.

3.3 HUAWEI CLOUD's Role under the PDPA

Personal data processed by HUAWEI CLOUD mainly includes customers' content data and personal information provided by customers when creating or managing their HUAWEI CLOUD accounts. As customers have full control over their content data, when processing personal data included in content data, HUAWEI CLOUD is generally regarded as the data processor. HUAWEI CLOUD acts as the data controller when dealing with personal data provided by the customers' set up or management of their HUAWEI CLOUD account.

HUAWEI CLOUD acts as the data controller of customers' personal data: When a customer performs operations on HUAWEI CLOUD platform, including but not limited to registering, purchasing services, real-name authentication and service support, HUAWEI CLOUD will collect some personal data, such as the customer's name, address, ID number, bank accounts, and others types of information according to the service used. HUAWEI CLOUD is ultimately responsible for the security and privacy protection of such customers' personal data, ensuring that the collection, processing and storage procedures comply with legal requirements, responding to data subjects' requests, complying with the PDPA requirements regarding limited disclosure, and finally taking actions to avoid data breaches.

HUAWEI CLOUD acts as the data processor of customer's content data: When customers use HUAWEI CLOUD services or applications on behalf of a controller to process

personal data included in their content, HUAWEI CLOUD is the data processor. HUAWEI CLOUD processes personal data on behalf of customers in accordance with personal data processing requirements or instructions from the data controller, and maintains records of data processing operations.

4

How HUAWEI CLOUD is Satisfying the Requirements of Thailand's PDPA

4.1 HUAWEI CLOUD Privacy Commitment

HUAWEI CLOUD has fully integrated cyber security and privacy protection into each cloud service providing and promising to provide customers with stable, reliable, secure, trustworthy, and evolvable services while respecting and protecting customers' privacy.

HUAWEI CLOUD solemnly treats and actively assumes corresponding responsibilities to comply with global privacy protection laws and regulations. HUAWEI CLOUD not only has set up professional privacy protection teams, but also develops and optimizes processes and new technologies, and continuously builds up privacy protection capabilities to achieve its own privacy protection objectives: strictly safeguarding services' boundaries, protecting customers' personal data security, and helping customers implement privacy protections.

4.2 HUAWEI CLOUD Basic Privacy Protection Principles

- **Lawfulness, Fairness and Transparency**
HUAWEI CLOUD processes personal data of data subjects lawfully, fairly and in a transparent manner.
- **Purpose Limitation**
HUAWEI CLOUD collects personal data for specific, explicit and lawful purposes and will not further process the data in a manner that is incompatible with those purposes.
- **Data Minimization**
When HUAWEI CLOUD processes personal data, personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed. Personal data will be anonymized or pseudonymized to the extent possible to reduce the risks for data subjects.
- **Accuracy**
HUAWEI CLOUD ensures that personal data is accurate and, when necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay depending on the purpose of data processing.
- **Storage Limitation**

Personal data will not be kept beyond the period necessary for the purposes of data processing.

- **Integrity and Confidentiality**

Taking into account the existing technical capabilities, implementation costs, and likelihood and severity of privacy risks, HUAWEI CLOUD processes personal data in a manner that ensures appropriate security of the personal data, including protection against accidental or unlawful destruction, loss, alteration, or unauthorized access and disclosure by using appropriate technical or organizational measures.

- **Accountability**

HUAWEI CLOUD is responsible for and able to demonstrate compliance with the preceding principles.

4.3 Basic Regulation Principles and HUAWEI CLOUD Related Practices

Based on the nature of HUAWEI CLOUD business and according to the requirements from Thailand's PDPA, data processors and data controllers have different obligations which HUAWEI CLOUD must acknowledge and fulfill accordingly.

When managing customers account information, HUAWEI CLOUD acts as the data controller:

Legal Obligation	Responsibilities of HUAWEI CLOUD as a Data Controller	HUAWEI CLOUD Response
Obtain Data Subject's Consent	Determining and controlling the time, method, purpose and source of personal data collection. Ensuring the purpose for data collection is disclosed to the relevant data subjects and used only for the consented purposes. When obtaining data from third parties, it is necessary to ensure that their source is legitimate and reliable as well as the data subject's consent was granted.	When registering an account, the customer is provided with the privacy statement and is asked for his consent. Data will be used or disclosed only for purposes agreed by the customer. When the scope or purpose for the collection of personal data changes, the privacy statement will be changed and customer's consent will be obtained again. If a service related to purchasing or after-sales involves the collection or the use of personal information for purposes other than those described in the privacy statement, an additional privacy statement shall be included within the related product agreement requiring data subjects' consent.
Secure Data Processing	HUAWEI CLOUD arranges appropriate security measures to prevent losses, unauthorized or illegal access, use, change and disclosure, and reviews	HUAWEI CLOUD has adopted strict administrative and technical controls to ensure personal data security in the access, transfer, storage, processing and other stages of personal data lifecycle. <ul style="list-style-type: none">• In terms of authentication, strict password policy and multi-factor

Legal Obligation	Responsibilities of HUAWEI CLOUD as a Data Controller	HUAWEI CLOUD Response
	<p>such measures when necessary or when technology changes.</p> <p>Security measures are generally carried out from the aspects of organization, management and technology:</p> <ul style="list-style-type: none"> • Identify the responsible person or team for internal information security; • Establish safety requirements according to their own situation; • Deploy security technologies to ensure the execution of security requirements. 	<p>authentication are adopted:</p> <ul style="list-style-type: none"> • In the aspect of permission management, role-based access control and permission management for operation and maintenance personnel is implemented; • In terms of data storage and transmission, sensitive data encryption is adopted; • In terms of data processing, monitoring and auditing of access to critical systems through logging and auditing of data processing is adopted. <p>Customers can also verify the privacy and security controls within HUAWEI CLOUD's environment through HUAWEI CLOUD security reports or certifications obtained. HUAWEI CLOUD has obtained multiple certifications from privacy compliance related international standard, including ISO 27701, ISO 29151, ISO 27018, BS 10012, SOC2 Type1, privacy audit reports (please refer to Chapter 6 for a detailed introduction of certifications). Among all the international standards, ISO27018 is the international code of conduct focusing on the protection of personal data regarding cloud, its adoption indicates that HUAWEI CLOUD has a complete personal data protection management system.</p> <p>Customers can also verify the privacy and security controls within HUAWEI CLOUD's environment through HUAWEI CLOUD security reports or certifications obtained. HUAWEI CLOUD has obtained multiple certifications from privacy compliance related international standard, including ISO 27701, ISO 29151, ISO 27018, BS 10012, SOC2 Type1, privacy audit reports (please refer to Chapter 6 for a detailed introduction of certifications). Among all the international standards, ISO27018 is the international code of conduct focusing on the protection of personal data regarding cloud, its adoption indicates that HUAWEI CLOUD has a complete personal data protection management system.</p>

Legal Obligation	Responsibilities of HUAWEI CLOUD as a Data Controller	HUAWEI CLOUD Response
Respond to Data Subject Rights	Communicating directly with the data subject on the collection and processing of their personal data. Responding to data subjects' requests and keeping records of any personal data processing. The response time and response to data subjects' requests shall meet the requirements stipulated by the PDPA.	<p>HUAWEI CLOUD provides customers with several communication channels to exercise their rights and formulate requests, including:</p> <ul style="list-style-type: none"> • Sending a request through the e-mail address indicated in the privacy statement; • Sending a request through the feedback page of HUAWEI CLOUD official website; • Sending a request through Data Subject Right Portal of HUAWEI CLOUD official website; • Sending a request through the service tickets page. <p>HUAWEI CLOUD will respond and process the request immediately after verifying the identity of the requestor.</p>
Record Processing Activities	Using collection and storage of logs solutions to record information on data subjects and data controllers, personal data collection purpose, personal data retention period, data subjects' requests and responses, and security control implementation operations.	<p>Retaining complete controls of any privacy management activities performed by HUAWEI CLOUD:</p> <ul style="list-style-type: none"> • Before a service is launched, a privacy impact assessment listing the type of personal data, their collection purpose and retention period shall be conducted. • According to regulatory requirements, when performing regular operations and maintenance on a service, any information such as the execution of security activities operational logs, data subject's requests and their related responses shall be retained.
Prevent Unauthorized Use Or Disclosure Of Data To Third Parties	HUAWEI CLOUD ensures the consent for the intended purpose from data subjects was acquired before using or disclosing personal data to a third party. If the third party is the data processor, it should be ensured that the parties have signed a personal data processing agreement clarifying the responsibilities and obligations of each party	<p>In its privacy statement, HUAWEI CLOUD describes the use of personal data and how to obtain the data subject's consent.</p> <p>To provide customers with the necessary transaction, service and security support, HUAWEI CLOUD may share some personal data with third parties. In such a case, HUAWEI CLOUD sign an agreement with the involved third parties stipulating personal data processing requirements. Such data processing requirements may include: personal data should not be used or stored for other purposes than the ones previously stated,</p>

Legal Obligation	Responsibilities of HUAWEI CLOUD as a Data Controller	HUAWEI CLOUD Response
	<p>and communication channels to be used.</p> <p>Ensuring the responsibilities listed in the PDPA are fulfilled.</p> <p>When transferring data to a third party, use a secure data transmission method to avoid data breach incident during transfer.</p>	<p>ensuring data security with appropriate technical and administrative controls, informing HUAWEI CLOUD in case of a data breach, and assisting in data subject's request response.</p> <p>When transferring personal data to a third party, HUAWEI CLOUD uses encrypted channels in order to ensure the personal data security.</p>
Data Erasure	<p>Personal data should be erased in a timely manner.</p> <p>Delete personal data when it becomes unnecessary.</p> <p>When the data subject makes a request for erasure, the corresponding data shall be deleted in accordance with related regulations.</p>	<p>HUAWEI CLOUD regularly reviews personal data collection, use, and disclosure purposes in order to anonymize, erase or perform other security processes on personal data that is no longer needed.</p> <p>Customers can close their accounts on the official website to extensively erase the data saved in HUAWEI CLOUD.</p>
Data Breach Notification	<p>Notify any personal data breach to the the Personal Data Protection Committee within 72 hours after becoming aware of the incident.</p>	<p>HUAWEI CLOUD has set up a 24/7 professional security incident response team. This team discloses personal data breaches in a timely manner in compliance with applicable laws and regulations and executes the adequate contingency plan and recovery process to reduce the impact on customers.</p>
Appoint a DPO	<p>Appointment of an internal personal data protection officer.</p>	<p>HUAWEI CLOUD's security management department has set up a DPO in each region, and the DPO is responsible for personal data protection in the region.</p>

When processing content data, HUAWEI CLOUD acts as the data processor:

Legal Obligation	Responsibilities of HUAWEI CLOUD as a Data Processor	HUAWEI CLOUD Response
Follow Instructions	<p>Performing activities related to the collection, use or disclosure of personal data according to the instructions provided</p>	<p>When providing customers with computing, storage, database, networking or other services, HUAWEI CLOUD provides the customer with several options to encrypt their content data while using</p>

Legal Obligation	Responsibilities of HUAWEI CLOUD as a Data Processor	HUAWEI CLOUD Response
	by the data controller.	those services. HUAWEI CLOUD cannot access or use customer's content data without their consent. Customers can control the entire life cycle of their content data in HUAWEI CLOUD and manage it according to their specific needs.
Secure Data Processing	<p>HUAWEI CLOUD arranges appropriate security measures to prevent losses, unauthorized or illegal access, use, change and disclosure, and reviews such measures when necessary or when technology changes.</p> <p>Security measures are generally carried out from the aspects of organization, management and technology:</p> <ul style="list-style-type: none"> • Identify the responsible person or team for internal information security; • Establish safety requirements according to their own situation; • Deploy security technologies to ensure the execution of security requirements. 	<p>HUAWEI CLOUD is mainly responsible for the security of the underlying cloud infrastructure as well as the privacy and security of their products:</p> <ul style="list-style-type: none"> • The underlying cloud infrastructure security: HUAWEI CLOUD infrastructure provides the best availability, complete customer isolation, and uses multiple data security technologies and related control measures such as identity authentication, access control, data transfer and storage encryption, recording and other means to guarantee the security of underlying cloud infrastructure. The powerful information security capabilities of the underlying cloud infrastructure lays a solid foundation for privacy and security on the cloud. • Customers can review HUAWEI CLOUD's security related certifications and reports such as, ISO 27001, CSASTAR gold, PCI-DSS and others to learn more about security controls in place. • Customers can review HUAWEI CLOUD's security related certifications and reports such as, ISO 27001, CSASTAR gold, PCI-DSS and others to learn more about security controls in place. • Products privacy: HUAWEI CLOUD deploys privacy protection controls along the product lifecycle from design to operations and maintenance. During the design thinking process, HUAWEI CLOUD analyzes the privacy requirements from relevant laws and regulations, and prioritize the security and privacy requirements when planning the product development; At

Legal Obligation	Responsibilities of HUAWEI CLOUD as a Data Processor	HUAWEI CLOUD Response
		<p>the product design stage, all types of personal data involved are sorted out and listed in order to identify potential risks through a Privacy Impact Assessment (PIA) and appropriate controls are implemented during the product design. At the development stage, HUAWEI CLOUD is ensuring the development process and code are conform to original privacy requirements through static code analysis and inspection; During the testing phase, all privacy features are rigorously tested and reviewed by a team of experts to ensure that privacy requirements and designs are well respected.</p> <ul style="list-style-type: none"> • Cloud service privacy protection compliance is not limited to the research and development stage. At the operations and maintenance stage, HUAWEI CLOUD ensures that personal data is not accessed and processed by any unauthorized party through various technical and administrative controls, so as to guarantee data subject's rights and ensure the privacy and security of any cloud service or product. • Customers can review HUAWEI CLOUD's privacy related certifications and reports such as, ISO 27701, ISO 29151, ISO 27018, and others to to verify the privacy controls in HUAWEI CLOUD's environment. • Customers can review HUAWEI CLOUD's privacy related certifications and reports such as, ISO 27701, ISO 29151, ISO 27018, and others to to verify the privacy controls in HUAWEI CLOUD's environment.
Data Breach Notification	Notify any personal data breach to the the Personal Data Protection Committee within 72 hours after becoming aware of the incident.	HUAWEI CLOUD has a dedicated team to ensure communication and contact with customers. In case of a data breach incident on the customers' side, HUAWEI CLOUD will cooperate with customers to investigate and respond adequately.
Record Processing	Using collection and storage of logs solutions	HUAWEI CLOUD has prepared and maintained records of personal data

Legal Obligation	Responsibilities of HUAWEI CLOUD as a Data Processor	HUAWEI CLOUD Response
Activities	to record information on data subjects and data controllers, personal data collection purpose, personal data retention period, data subjects' requests and responses, and security control implementation operations.	<p>processing activities in accordance with the rules and methods set forth by the PDPA:</p> <ul style="list-style-type: none">• Before the launch of a service involving personal data, HUAWEI CLOUD will perform a privacy impact assessment, which will list within the assessment not only the type of personal data but also their respected purpose of collection and retention period.• After the launch of a service involving personal data, when customers request HUAWEI CLOUD to provide assistance to data subject right response and fault handling, HUAWEI CLOUD will keep records of its own operations.

5

How HUAWEI CLOUD Supports Customers to Comply with Thailand's PDPA

5.1 Customers' Privacy Protection Responsibilities and Obligations

When the customer is the data controller and HUAWEI CLOUD provides assistance in processing personal data in the customer's content data, the customer is likely to fall within the PDPA's jurisdiction. If he does, the customer shall bear the privacy protection responsibilities stated by the PDPA, and HUAWEI CLOUD will do its best to help the customer achieve security and privacy compliance with the PDPA.

Legal Obligation	Customer's Responsibilities when Acting as the Data Controller	How HUAWEI CLOUD Can Help
Obtain Data Subject's Consent	Determining and controlling the time, method, purpose and source of personal data collection, and decide whether to store or process personal data in HUAWEI CLOUD. The customer needs to ensure that the purpose for data collection is disclosed to the relevant data subjects and used only for the consented purposes. When obtaining data from third parties, it is necessary to ensure that their source is legitimate and reliable as well as the data subject's consent was granted.	Some of HUAWEI CLOUD's products and services provide functions or capabilities that better fulfill the requirements of privacy protection laws on informing data subjects. For example, customers can use HUAWEI CLOUD's interface to upload their privacy policy and records relevant operations.
Secure Data Processing	HUAWEI CLOUD arranges appropriate security measures to prevent losses, unauthorized or illegal access, use, change and disclosure, and reviews such measures when necessary or when technology changes. Security measures are generally carried out from the aspects of organization,	HUAWEI CLOUD provides access control, network isolation and other security configuration. HUAWEI CLOUD provides specialized security products to help customers improve their

Legal Obligation	Customer's Responsibilities when Acting as the Data Controller	How HUAWEI CLOUD Can Help
	<p>management and technology:</p> <ul style="list-style-type: none"> Identify the responsible person or team for internal information security; Establish safety requirements according to their own situation; Deploy security technologies to ensure the execution of security requirements. The customer can use the security configuration provided by HUAWEI CLOUD, or use his own security tools or from a third party. 	<p>security capabilities in certain domains, such as Identity and Access Management, Cloud Eye Service, Database Security Service, Data Encryption Workshop, Web Application Firewall, Advanced Anti-DDoS, Vulnerability Scan Service, Virtual Private Network, Virtual Private Cloud, Virtual Private Cloud etc.</p> <p>HUAWEI CLOUD provides specialized security products to help customers improve their security capabilities in certain domains, such as Identity and Access Management, Cloud Eye Service, Database Security Service, Data Encryption Workshop, Advanced Anti-DDoS, Vulnerability Scan Service, Virtual Private Network, etc.</p>
Respond to Data Subject Rights	<p>Communicating directly with the data subject on the collection and processing of their personal data. Responding to data subjects' requests and keeping records of any personal data processing. The response time and response to data subjects' requests shall meet the requirements stipulated by the PDPA.</p>	<p>HUAWEI CLOUD has a dedicated team to ensure communication with customers. In case of a data breach incident, HUAWEI CLOUD will cooperate with customers to provide logs and records according to the provisions stated in the data processing agreement.</p> <p>HUAWEI CLOUD has a dedicated team to ensure communication with customers. Customers can seek assistance from HUAWEI CLOUD through the service ticket page.</p>
Record Processing Activities	<p>Using collection and storage of logs solutions to record information on data</p>	<p>HUAWEI CLOUD provides Log Tank</p>

Legal Obligation	Customer's Responsibilities when Acting as the Data Controller	How HUAWEI CLOUD Can Help
	subjects and data controllers, personal data collection purpose, personal data retention period, data subjects' requests and responses, and security control implementation operations.	Service , Cloud Trace Service , Volume Backup Service , Cloud Server Backup Service to help customers collect and analyze logs conveniently, and identify privacy risks in time. HUAWEI CLOUD provides Log Tank Service , Cloud Trace Service , Volume Backup Service , Cloud Server Backup Service to help customers collect and analyze logs conveniently, and identify privacy risks in time.
Prevent Unauthorized Use or Disclosure of Data to Third Parties	HUAWEI CLOUD ensures the consent for the intended purpose from data subjects was acquired before using or disclosing personal data to a third party. If the third party is the data processor, it should be ensured that the parties have signed a personal data processing agreement clarifying the responsibilities and obligations of each party and communication channels to be used. Ensuring the responsibilities listed in the PDPA are fulfilled. When transferring data to a third party, use a secure data transmission method to avoid data breach incident during transfer.	-
Data Erasure	Personal data should be erased in a timely manner. Delete personal data when it becomes unnecessary. When the data subject makes a request for erasure, the corresponding data shall be deleted in accordance with related regulations.	HUAWEI CLOUD offers the function to erase personal data from its services and products.
Data Breach Notice	Notify any personal data breach to the the Personal Data Protection Committee within 72 hours after becoming aware of the incident.	HUAWEI CLOUD has a dedicated team to ensure communication with customers. In case of a data breach incident, HUAWEI CLOUD will cooperate with customers

Legal Obligation	Customer's Responsibilities when Acting as the Data Controller	How HUAWEI CLOUD Can Help
		to provide logs and records according to the provisions stated in the data processing agreement. HUAWEI CLOUD has a dedicated team to ensure communication with customers. Customers can seek assistance from HUAWEI CLOUD through the service ticket page.
Appoint a DPO	Appointment of an internal personal data protection officer.	-
Appoint a Representative	If the data controller is not located in Thailand, a local representative of the data controller shall be designated in writing. The representative must be in Thailand and be authorized to act on behalf of the data controller without any limitation of liability with respect to the collection, use or disclosure of the personal data according to the purposes set by the data controller.	-

5.2 How HUAWEI CLOUD Products and Services Help Customers Implementing Content Data Privacy and Security

HUAWEI CLOUD has a deep understanding of the importance of customers' privacy protection needs, combining it with its own privacy protection practices and technical capabilities in order to help customers to achieve compliance with the PDPA leveraging HUAWEI CLOUD products and services. HUAWEI CLOUD provides customers with a large range of products and services such as networking products, database products, security products, solutions for management and deployment as well as other products. Data protection, data deletion, network isolation, rights management and other functions implemented in HUAWEI CLOUD products can help customers implement privacy and security of content data.

- **Management and Deployment Products**

Product	Description	Corresponding privacy protection obligations

Product	Description	Corresponding privacy protection obligations
Identity and Access Management (IAM) Identity and Access Management (IAM)	<p>Identity and Access Management (IAM) provides identity authentication and permissions management. With IAM, customers can create users for employees, applications, or systems in their organization, and control the users' permissions on owned resources.</p> <p>Through IAM, customers can perform user management, identity authentication, and fine-grained resource access control on the cloud to prevent unauthorized modification of content data.</p>	Secure Data Processing
Cloud Trace Service (CTS) Cloud Trace Service (CTS)	<p>Customers can review logs to perform security analysis, track resource changes, audit compliance, and locate issues, etc.</p> <p>Customers can configure CTS object storage service to save operation records to CTS in real time, save operation records for a long period, protect the right to know of data subjects, and enable quick searching.</p>	Record Processing Activities
Cloud Eye Service (CES) Cloud Eye Service (CES)	<p>Providing customers with a multidimensional monitoring platform for elastic cloud servers, bandwidth and other resources.</p> <p>Through "Cloud Eye", customers can have a comprehensive understanding of HUAWEI CLOUD resources usage and business operations status, and respond to alarms in time to ensure business continuity.</p>	Secure Data Processing
Log Tank Service (LTS) Log Tank Service (LTS)	<p>Providing functions such as log collection, real-time query and storage, which can be used to make real-time decision analysis, improve the efficiency of log processing, and help customers to cope with daily operations and maintenance scenarios such as real-time logs collection and query analysis without development's requirements.</p> <p>Customers can keep records of operations on personal data through LTS to guarantee the data subjects' right to know.</p>	Record Processing Activities

- **Security Products**

Product	Description	Corresponding privacy protection obligations
Database Security Service (DBSS) Database Security Service (DBSS)	<p>Database Security Service (DBSS) uses machine learning mechanism and big data technologies to protect customers' databases on the cloud, audit and detect risky behaviors, such as SQL injection, operational risks identification, etc.</p> <p>Customers can use DBSS to detect potential risks and ensure the security of their databases.</p>	Secure Data Processing
Data Encryption Workshop (DEW) Data Encryption Workshop (DEW)	<p>Data Encryption Workshop (DEW) is a full-stack data encryption service. It covers Key Management Service (KMS), Key Pair Service (KPS), and Dedicated HSM. With DEW, customers can develop customized encryption applications, and integrate it with other HUAWEI CLOUD services to meet the most demanding encryption scenarios. Customers can also use the service to develop their own encryption applications.</p> <p>Customers can use DEW for centralized key lifecycle management to ensure the integrity of data storage procedures.</p>	Secure Data Processing
Web Application Firewall (WAF) Web Application Firewall (WAF)	<p>Web Application Firewall (WAF) can conduct multi-dimensional detection and protection of website traffic, combining with deep machine learning to identify malicious requests, protect against unknown threats, and block common attacks such as SQL injection or cross-site scripting.</p> <p>Customers can use WAF to protect their websites or servers from external attacks that affect the availability, security, or unwanted additional resources consumption of their web applications, reducing the risk of data tampering and theft.</p>	Secure Data Processing
Vulnerability Scan Service (VSS) Vulnerability Scan Service (VSS)	<p>Vulnerability Scan Service (VSS) is a multi-dimensional security detection service, with five core functions: web vulnerability scanning, asset content compliance detection, configuration baseline scanning, operating system vulnerability scanning, and identification of systems with a weak password.</p> <p>VSS enables customers to protect their data</p>	Secure Data Processing

Product	Description	Corresponding privacy protection obligations
	integrity by automatically identifying security threats on their exposed websites or servers.	
Advanced Anti-DDoS (AAD) Advanced Anti-DDoS (AAD)	Advanced Anti-DDoS (AAD) is a value-added security defense service that defends against large volumetric DDoS attacks on Internet servers. Customers can configure AAD to divert the attack traffic to high-defense IP addresses with significant defense capabilities for scrubbing, keeping customers' business stable and reliable.	Secure Data Processing

- Network Products**

Product	Description	Corresponding privacy protection obligations
Virtual Private Network (VPN) Virtual Private Network (VPN)	Virtual Private Network (VPN) establishes a flexible, scalable IPsec encrypted communication channel between customers' local data center and their VPC on HUAWEI CLOUD. Customers can build a flexible and scalable hybrid cloud computing environment, and improve their security posture with encryption of the communication channel.	Secure Data Processing
Virtual Private Cloud (VPC) Virtual Private Cloud (VPC)	Virtual Private Cloud (VPC) enables customers to create private, isolated virtual networks on HUAWEI CLOUD. Customers can configure IP address ranges, subnets, and security groups, assign Elastic IP (EIP) addresses, and allocate bandwidth in a VPC. VPC is the customer's private network on the cloud, with 100% isolation from other customers, enhancing the data security on the cloud.	Secure Data Processing

- Storage Products**

Product	Description	Corresponding privacy protection obligations
---------	-------------	--

Product	Description	Corresponding privacy protection obligations
Volume Backup Service (VBS) Volume Backup Service (VBS)	<p>Volume Backup Service (VBS) creates online permanent incremental backup for cloud hard disk, automatically encrypts the backup disk data, and can restore the data to any backup point to enhance data availability.</p> <p>VBS can reduce the possibility of virus attack, human error deletion as well as hardware or software failure, protect data security and reliability, and reduce the risk of data tampering.</p>	Record Processing Activities
Cloud Server Backup Service (CSBS) Cloud Server Backup Service (CSBS)	<p>Cloud Server Backup Service (CSBS) can simultaneously create a consistent online backup of multiple cloud drives within the cloud server.</p> <p>CSBS can reduce the possibility of virus attack, human error deletion as well as hardware or software failure, protect data security and reliability, and reduce the risk of data tampering.</p>	Record Processing Activities

6

HUAWEI CLOUD Privacy Protection Related Certifications

HUAWEI CLOUD complies with all applicable privacy laws and regulations in the place where it operates. HUAWEI CLOUD has a professional legal team to closely monitor the update of laws and regulations, continuously track and analyze global laws and regulations, and ensure compliance with applicable laws and regulations.

HUAWEI CLOUD's capabilities and achievements in privacy protection and personal data security have been widely recognized worldwide by third-party certifications. Up to now, HUAWEI CLOUD has obtained almost 20 certifications from more than ten organizations inside and outside China, including regional certifications on data security and global standard certifications related to privacy and data security.

Privacy Related Standard Certifications:

- **ISO 27701**
Privacy information management system certification. The ISO 27701 certification shows that HUAWEI CLOUD has established a solid management system related to data privacy protection.
- **ISO 29151**
International practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
- **ISO 27018**
International code of conduct focused on the protection of personal data in Cloud. The adoption of ISO 27018 indicates that HUAWEI CLOUD has met the requirements of an internationally recognized personal data protection measures of public cloud platform, and can guarantee the security of customers' personal data.
- **BS 10012**
Personal information data management system standard issued by the British Standards Institute (BSI). The BS 10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
- **SOC2 Audit**
An independent audit report issued by a third party audit institution based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers. At present, HUAWEI CLOUD has passed the audit of SOC2 type 1 Privacy Principle, which proves that

HUAWEI CLOUD has reasonable control measures in terms of cloud management and technology.

Data Security Standard Certifications:

- ISO 27001 Information Security Management System Certification
- ISO 27017 Cloud Service Information Security Management System
- ISO 20000 Information Technology Service Management System Certification
- ISO 22301 Business Continuity Management System, CSA STAR Cloud Security International Gold Certification
- PCI DSS Third-Party Payment Industry Data Security Standard Certification
- International Common Criteria (CC) EAL3+ Security Assessment Standard

Regional Security Certifications:

- Multi-Tier Cloud Security(MTCS) Level3 (Singapore)
- Certification for the Capability of Protecting Cloud Service User Data (China)
- Trusted Cloud Service (China)
- Classified Cybersecurity Protection of China's Ministry of Public Security (China)
- Gold Operations and Management certification (China)
- Cloud Service Security Certification by Cyberspace Administration of China (China)
- ITSS Cloud Computing Service Capability Evaluation by the Ministry of Industry and Information Technology (China).

7 Conclusion

HUAWEI CLOUD always adheres to HUAWEI's "customer-centric" core values, fully understands the importance of customer personal security, and respects and protects customer privacy rights. HUAWEI CLOUD has industry-leading security and privacy protection technologies and provides customers with capabilities through cloud services and solutions to help customers cope with increasingly complex and open network environments and increasingly strict privacy protection laws and regulations.

To satisfy the requirements of local privacy protection laws and regulations, HUAWEI CLOUD follows up on the updates of relevant laws and regulations, converting new requirements into internal HUAWEI CLOUD regulations, and optimizing internal processes to ensure that all activities carried out by HUAWEI CLOUD meet the requirements of laws and regulations. HUAWEI CLOUD continuously develops and launches privacy protection related services and solutions to help customers implement privacy protection laws and regulations in each region.

Compliance with protection laws and regulations is a long-term and multi-disciplinary activity. HUAWEI CLOUD is committed to continuously improving capabilities in the future in order to satisfy relevant laws and regulations and to build a secure and trustworthy cloud platform for customers.

This white paper is for reference only and does not have any legal effect or constitutes a legal advice. Customers should assess their use of cloud services as appropriate and ensure compliance with the PDPA of Thailand when using HUAWEI CLOUD.

8

Version History

Date	Version	Description
August 2024	2.2	Routine Update
June 2022	2.1	The Thailand PDPA came in to force.
April 2022	2.0	Compliance requirement update
August 2020	1.0	First release