

# HUAWEI CLOUD Compliance with Singapore

Issue	1.0
Date	2023-04-11



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. 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 the property 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

---

<b>1 Overview.....</b>	<b>1</b>
1.1 Scope of Application.....	1
1.2 Purpose of Publication.....	1
1.3 Basic Definition.....	1
<b>2 Privacy Protection Responsibilities.....</b>	<b>3</b>
<b>3 Overview of Singapore Privacy Regulations.....</b>	<b>5</b>
3.1 Background of Regulations.....	5
3.2 Role Division and Basic Obligations.....	5
3.3 HUAWEI CLOUD's Role under Singapore's Privacy Regulation.....	6
<b>4 How HUAWEI CLOUD Responses to the Singapore's Privacy Compliance Requirements.....</b>	<b>8</b>
4.1 HUAWEI CLOUD Privacy Commitment.....	8
4.2 HUAWEI CLOUD Basic Privacy Protection Principles.....	8
4.3 Compliance Measures of HUAWEI CLOUD in Response to Singapore's Personal Data Protection Act, Personal Data Protection Ordinance, and Personal Data Protection (Data Breach Notification) Ordinance .....	9
<b>5 HUAWEI CLOUD Assists Customers in Responding to Singapore Privacy Compliance Requirements.....</b>	<b>20</b>
5.1 Customer's Privacy Protection Responsibilities.....	20
5.2 HUAWEI CLOUD Products and Services Help Customers Implement Content Data Privacy and Security .....	32
<b>6 HUAWEI CLOUD Privacy Protection Related Certifications.....</b>	<b>39</b>
<b>7 Conclusion.....</b>	<b>41</b>
<b>8 Version History.....</b>	<b>42</b>

# 1 Overview

---

## 1.1 Scope of Application

This document provides information applicable to the products and services of HUAWEI CLOUD in Singapore and the country (referred to as "Singapore").

## 1.2 Purpose of Publication

This document is intended to help customers understand:

- 1) HUAWEI CLOUD privacy protection responsibility model;
- 2) Legal requirements related to privacy in Singapore;
- 3) Based on the responsibility model, HUAWEI CLOUD's own compliance with Singapore's privacy regulations;
- 4) HUAWEI CLOUD's achieved control and effectiveness in privacy management;
- 5) Based on the liability model, the responsibilities and obligations that customers under the jurisdiction of the Singapore Privacy Regulations must follow;
- 6) How to use HUAWEI CLOUD security products or services to achieve privacy compliance.

## 1.3 Basic Definition

- **Data controller/organization:** includes any individual, company, association or body, whether legal or unincorporated, whether or not incorporated or recognized under the laws of Singapore, whether or not it is a resident of Singapore or has an office or place of business in Singapore. The above description comes from the "Singapore Personal Data Protection Act" (hereinafter referred to as "PDPA"), which also refers to the "data controller" in this article.
- **Data processor/data intermediary:** An organization that processes personal data on behalf of another organization , excluding employees of that

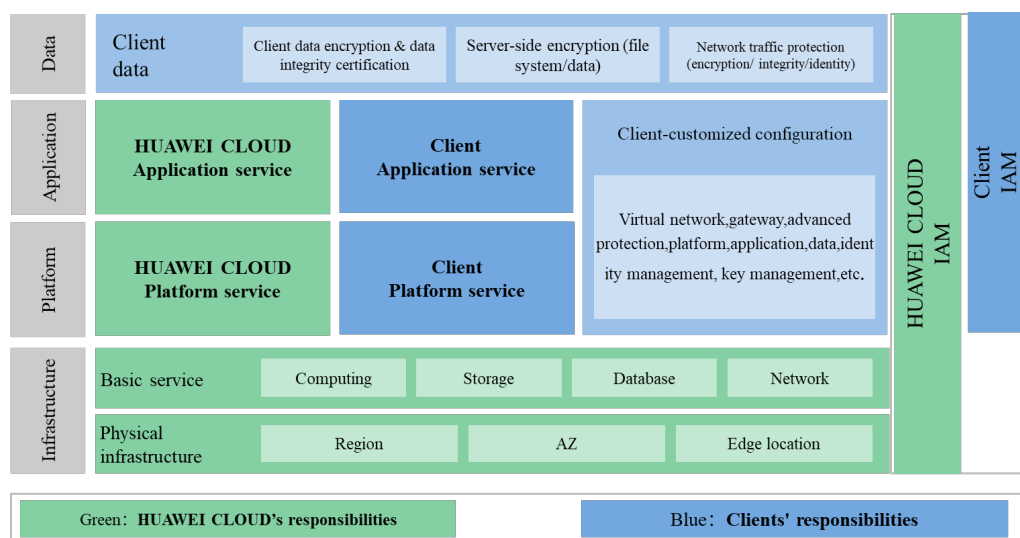
organization . The above description comes from the PDPA, which also refers to the "data processor" in this article.

- **Content data:** refers to the data stored or processed by customers during the use of HUAWEI CLOUD services, including but not limited to data, files, software, images, audio, video, and other types of data.
- **Collection:** Refers to any single act or series of actions involved in an organization gaining control over or possessing personal data.
- **Processing:** in relation to personal data, means any operation or series of operations relating to personal data, including recording, holding, organizing, adaptation or alteration, restoration, combination, transmission, erasure or destruction.
- **Use:** refers to any act or a series of acts by which an organization uses personal data.
- **Disclosure:** Any single or series of actions by an organisation that disclose, transfer or otherwise provide to any other organisation personal data under its control or possession.
- **Personal data:** any information relating to an identifiable or identifiable natural person ("data subject"). An identifiable natural person is a person whose identity can be identified directly or indirectly by means of an identifier such as name, identification number, location data, or by one or more specific factors related to the physical, physiological, mental, economic, cultural or social identity of the natural person. Personal data includes the email address, phone number, biometric feature (fingerprint), location data, IP address, medical information, religious belief, social security number, and marital status of a natural person.
- **HUAWEI CLOUD:** HHUAWEI's cloud service brand, dedicated to providing stable, reliable, secure, reliable, and innovative cloud services.
- **Customer:** Registered users who have entered into business relationships with HUAWEI CLOUD.

# 2 Privacy Protection Responsibilities

Due to the complex cloud service business model, the privacy protection of personal data is not the sole responsibility of one single party, but requires the joint effort 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 should 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 should 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 should notify both regulatory authorities and Data Subjects, and take adequate actions in accordance with regulatory requirements.

# 3

## Overview of Singapore Privacy Regulations

---

### 3.1 Background of Regulations

The Personal Data Protection Act (PDPA) provides a baseline standard for personal data protection in Singapore, regulates the collection, use, and disclosure of personal data, and guarantees the right to protect personal data. It also recognizes the need for data controllers to collect, apply and disclose personal data for reasonable purposes. In November 2020, the Personal Data Protection Act was fully revised for the first time and the Personal Data Protection (Amendment) Act 2020 was formally promulgated. The requirements of the amendment go into effect in phases, and the amendments that take effect in February 2021 include a notification requirement for data breaches, an expansion of the scope of express consent, and exceptions to express consent. The amendments, which take effect in October 2022, include an increase in the amount of fines for organizations violating the requirements of the PDPA.

### 3.2 Role Division and Basic Obligations

Singapore's privacy regulations define two key roles: organization (data controller) and data intermediary (data processor).

**Organization (Data Controller):** includes any individual, company, association or body, whether legal or unincorporated, whether incorporated or recognized under the laws of Singapore, whether resident of Singapore or having an office or place of business in Singapore.

**Data broker (data processor):** An organization that processes personal data on behalf of another organization, but does not include employees of that organization.

The basic obligations of a **data controller** include:

1. **Notification and consent:** The data controller notifies individuals in advance of the purpose of collecting, using, or disclosing personal data. The data controller may only collect, use or disclose personal data for the purpose of

the individual's consent or as authorized by the PDPA or any other written law of Singapore. If an individual withdraws consent, the data controller must cease collecting, using or disclosing personal data.

2. **Purpose limitation:** The purpose limitation obligation stipulates that the data controller may collect, use, or disclose personal data only for reasonable purposes that have been notified to the individual.
3. **Access and correction:** Individuals have the right to request access to their personal data and to correct their personal data in the possession or under the control of a data controller.
4. **Accuracy:** The PDPA requires data controllers to ensure that personal data collected by or on behalf of the controller is accurate and complete, so that all relevant and accurate personal data can be taken into account when personal data may be used to make decisions that affect individuals.
5. **Protection:** Before collecting, using, or disclosing personal data, the data controller must evaluate the data to ensure that the data collection, use, or disclosure will not adversely affect the data. Protect personal data in its possession or control by making reasonable security plans to prevent unauthorized access to, collection, use, disclosure, copying, modification, disposal and loss or similar risks of the medium or device on which the personal data is stored.
6. **Retention restriction:** When the data controller is no longer able to meet the purpose for which personal data is collected and personal data is no longer required to be retained for legal or commercial purposes, stop retaining personal data or ensure that the data cannot identify individuals.
7. **Transfer restriction:** The data controller shall not transfer any personal data to a country or region outside Singapore unless the protection of the transferred personal data complies with the data protection standards specified in the PDPA.
8. **Notification of a breach:** The data controller must assess in a reasonable and expeditious manner whether a data breach should be notified and, where assessed as notifiable, notify the affected individuals and/or the Commission.
9. **Accountability obligations:** Accountability obligations mainly refer to the policies and practices necessary for data controllers to formulate and implement PDPA obligations and are available to the public. Related requirements are collectively referred to as accountability obligations in PDPA.

### 3.3 HUAWEI CLOUD's Role under Singapore's Privacy Regulation

Personal data processed by HUAWEI CLOUD mainly includes personal data in customer content data and personal data provided by customers during operations including but not limited to registration, service purchase, real-name authentication, and service support on HUAWEI CLOUD. Customers have control over content data. HUAWEI CLOUD processes personal data in content data. HUAWEI CLOUD acts as the data controller of personal data when processing personal data provided by customers who create or manage HUAWEI CLOUD accounts.

HUAWEI CLOUD acts as the controller of personal data.

When a customer uses HUAWEI CLOUD to perform operations, including but not limited to registration, service purchase, real-name authentication, and service support, HUAWEI CLOUD collects personal data from the customer for customer service purposes, including the name, address, certificate number, and bank account information. HUAWEI CLOUD will be responsible for the security and privacy protection of the customer's personal data based on Singapore privacy regulations, ensure that the collection, processing, storage, and transmission of personal data comply with laws and regulations, and respond to personal data subjects' rights applications.

HUAWEI CLOUD serves as the processor/service provider of personal data of customer content data.

When a customer is the controller of personal data and uses HUAWEI CLOUD services or applications to process personal data in its content data, HUAWEI CLOUD is the personal data processor or service provider. HUAWEI CLOUD processes personal data on behalf of customers in accordance with personal data processing agreements or instructions from personal data controllers.

# 4

## How HUAWEI CLOUD Responses to the Singapore's Privacy Compliance Requirements

---

### 4.1 HUAWEI CLOUD Privacy Commitment

HUAWEI CLOUD has placed cyber security and privacy protection as top priorities. 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 determined, 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 should 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 Compliance Measures of HUAWEI CLOUD in Response to Singapore's Personal Data Protection Act, Personal Data Protection Ordinance, and Personal Data Protection (Data Breach Notification) Ordinance**

Based on the features of HUAWEI CLOUD services and the requirements of Singapore's Personal Data Protection Act, Personal Data Protection Ordinance, and Personal Data Protection (Data Breach Notification) Ordinance, HUAWEI CLOUD, as a legal entity that processes personal data, acts as a data controller in different scenarios.

HUAWEI CLOUD actively responds to and fulfills its obligations by adopting the following privacy protection mechanisms and technologies to comply with the requirements of Singapore's Personal Data Protection Act, Personal Data Protection Ordinance, and Personal Data Protection (Data Breach Notification) Ordinance. The following specific requirements applicable to HUAWEI CLOUD incorporate legal requirements and supplementary notes of regulations.

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Notice and Consent	<ol style="list-style-type: none"><li>1. The data controller shall notify individuals in advance of the purposes for which personal data is collected, used or disclosed.</li><li>2. The data controller may only collect, use or disclose personal data for the purpose of the individual's consent or under the authorization of the PDPA or any other written law of Singapore.</li><li>3. If an individual withdraws consent, the data controller must cease collecting, using, or disclosing personal data.</li></ol>	<ol style="list-style-type: none"><li>1. If the customer's personal data needs to be collected during interaction with HUAWEI CLOUD, HUAWEI CLOUD will proactively notify the collected personal data type, purpose, processing method, and time, such as the <a href="#">HUAWEI CLOUD Privacy Policy Statement</a> provided on the official website. If personal data needs to be collected in various offline marketing activities, provide a privacy notice in a prominent position and provide a consent option when personal data is collected.</li><li>2. HUAWEI CLOUD will not use or disclose customer content data unless authorized by the customer or to comply with local laws and regulations or binding orders from government agencies.</li></ol>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Purpose Limitation	1. A data controller may collect, use or disclose personal data only for reasonable purposes for which individuals have been notified.	<p>1. HUAWEI CLOUD collects the customer's personal data necessary for providing services only after obtaining the customer's consent and processes the customer's personal data within the scope specified in the <a href="#">Privacy Policy Statement</a>.</p> <p>2. In the HUAWEI CLOUD product design phase, HUAWEI CLOUD will sort out all involved personal data types and perform a privacy impact assessment (PIA) to ensure that the personal data collected by HUAWEI CLOUD products does not exceed the requirements for the purpose. During O&amp;M, HUAWEI CLOUD sets different access permissions for personal data based on employees' roles to ensure that the personal data that employees can access or use is only necessary for their work.</p>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Access and Correction	1. Individuals have the right to request access to their personal data and to correct their personal data in the possession or under the control of a data controller.	<p>1. HUAWEI CLOUD guarantees customers the right to access and correct their personal data as a data subject. HUAWEI CLOUD has established a response mechanism to data subjects' rights requests to ensure that data subjects' rights requests are properly and promptly responded to.</p> <p>2. HUAWEI CLOUD will accurately and completely respond to the data subject's request and provide copies of personal data use and disclosure information to the data subject in the form of documents.</p>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Accuracy	1. The personal data collected by the data controller is accurate and complete to ensure that all relevant and accurate personal data can be taken into account when personal data may be used to make decisions that affect individuals.	1. HUAWEI CLOUD takes different measures to ensure the accuracy of customer personal data. For example, HUAWEI CLOUD verifies the validity of personal data entered by customers to enhance the standardization and accuracy of data input. HUAWEI CLOUD also requires the customer to enter the verification code obtained from the email address or mobile number provided by the customer to confirm the customer's identity and the accuracy of related contact information. HUAWEI CLOUD provides customers with multiple data security and privacy protection functions to ensure the accuracy of their content data.

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Protecting	<p>1. Before collecting, using, or disclosing personal data, the data controller shall make an assessment to ensure that the behavior will not adversely affect the individual. Protect personal data in its possession or control by making reasonable security plans to prevent unauthorized access to, collection, use, disclosure, copying, modification, disposal and loss or similar risks of the media or devices on which the personal data is stored.</p>	<p>1. To effectively identify and control privacy risks, HUAWEI CLOUD extensively analyzes and manages privacy risks in various cloud services. Privacy Impact Assessment (PIA) must be performed before personal data is processed. It mainly includes identifying personal data items involved in services, business scenarios and handling processes, compliance analysis, possible impact on data subjects, risk analysis, risk control measures and plans, and incorporating all privacy risk control requirements into the design solution. Do business only if privacy risks are reduced to an acceptable level.</p> <p>2. HUAWEI CLOUD uses a series of technologies to ensure the security of customers' personal data. For example, identity authentication and access control technologies are used to implement role-based policies with minimum permissions to prevent unauthorized processing of personal data. Encryption technologies are widely used to encrypt customers' personal data for storage and transmission, ensuring the security of personal data storage and transmission. Log</p>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
		<p>recording and audit technologies are used to detect potential security risks in a timely manner, providing feedback and solving problems in a timely manner.</p> <p>3. HUAWEI CLOUD uses various data security technologies and related control measures, such as identity authentication and access control, data transmission and storage encryption, and log recording, to ensure the security of HUAWEI CLOUD services.</p>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Retention Limits	1. When the data controller is no longer able to meet the purpose for which personal data was collected and personal data is no longer required to be retained for legal or commercial purposes, stop retaining personal data or ensure that the data cannot identify individuals.	<p>1. HUAWEI CLOUD will retain the customer's personal data for the period required to achieve the purpose specified in the privacy statement, unless the retention period is extended according to laws and regulations. The retention period may vary based on the purpose of the processing and the associated service. After the customer deregisters the account, HUAWEI CLOUD stops providing services to the customer and deletes the customer's personal data.</p> <p>2. If the customer proactively deletes the customer's content data or needs to delete the data due to the expiration of the service, HUAWEI CLOUD will strictly comply with applicable laws and regulations and the agreement with the customer, and delete the customer's data according to the data destruction standards.</p>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Transfer Restriction	1. The data controller shall not transfer any personal data to a country or territory outside Singapore unless the protection of the transferred personal data complies with the data protection standards specified in the PDPA.	1. HUAWEI CLOUD has established data centers in multiple countries around the world. When cross-border data transmission is required during O&M, HUAWEI CLOUD complies with local privacy protection laws and regulations and passes strict internal review. If cross-border data transfer is performed after a data transfer agreement is signed or the explicit consent of the data subject is obtained, ensure that personal data is processed in a legal, proper, and transparent manner.

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Leakage Notice	1. The data controller must assess in a reasonable and expeditious manner whether a data breach should be notified and, where assessed as notifiable, notify the client, who informs the affected individuals and/or the committee.	1. HUAWEI CLOUD has developed a comprehensive personal data breach management system. Relevant personnel will analyze the impact of the incident based on the process. If the incident has affected or will affect cloud service customers, HUAWEI CLOUD will initiate a notification mechanism to notify the committee and customers of the incident. The notification content includes but is not limited to the incident description, cause, impact, measures taken by HUAWEI CLOUD, and measures recommended by the customer. In addition, HUAWEI CLOUD has set up a 24/7 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations. In addition, the emergency plan and recovery process are executed to reduce the impact on services.

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Accountability obligations	<ol style="list-style-type: none"><li>1. Data controllers need to develop and implement the policies and practices necessary to implement PDPA obligations and make them known to the public. Specific requirements for this obligation include:</li><li>2. Employees should be aware of such policies and practices; The data controller should establish a process for responding to complaints related to the Personal Data Protection Act, and the complaint method should be known to the public. The data controller shall have dedicated personnel responsible for PDPA compliance and publicizing relevant contact information.</li></ol>	<ol style="list-style-type: none"><li>1. Huawei has developed and implemented policies and regulations on personal data protection. HUAWEI CLOUD complies with the same policies as Huawei and has established a comprehensive privacy protection process system to ensure that business activities comply with privacy protection requirements through a series of scientific and strict processes. such as the privacy process framework, protection policies, and privacy protection design specifications. Huawei's personal data protection policies and regulations are visible to all employees on Huawei's intranet. If there is any policy change, Huawei will notify employees to ensure that employees are aware of and comply with relevant policies and ensure the security of customer personal data through internal management.</li></ol>

# **5 HUAWEI CLOUD Assists Customers in Responding to Singapore Privacy Compliance Requirements**

---

## **5.1 Customer's Privacy Protection Responsibilities**

When a customer uses HUAWEI CLOUD services to provide services under the jurisdiction of Singapore's privacy regulations for other electronic system users, HUAWEI CLOUD will assist the customer in fulfilling its obligations.

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Notice and Consent	<ol style="list-style-type: none"> <li>1. The data controller shall notify individuals in advance of the purposes for which personal data is collected, used or disclosed.</li> <li>2. The data controller may only collect, use or disclose personal data for the purpose of the individual's consent or under the authorization of the PDPA or any other written law of Singapore.</li> <li>3. If an individual withdraws consent, the data controller must cease collecting, using or disclosing personal data.</li> </ol>	<ol style="list-style-type: none"> <li>1. The customer's content data in HUAWEI CLOUD contains personal data. The customer shall inform data subjects of the purpose of personal data collection and obtain their consent. The data subject may send a reasonable request to withdraw the consent deemed to have been given. In addition, customers can use functions provided by HUAWEI CLOUD products and services or capabilities built by themselves to better implement the notice and consent principles specified in the personal data protection law. For example, in HUAWEI CLOUD <b>Convergent Video Cloud Service (CVCS)</b>, customers can use the interfaces for signing and querying privacy notices to embed the functions of consenting to or withdrawing privacy notices and recording related operations to notify users of personal data processing policies. For cloud services that involve personal data processing, customers can take privacy protection measures based on the information about personal data types, processing, and storage methods provided in HUAWEI</li> </ol>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
		CLOUD product documentation.
Purpose Limitation	1. A data controller may collect, use or disclose personal data only for reasonable purposes for which individuals have been notified.	1. If the customer's content data in HUAWEI CLOUD contains personal data, the customer can rely on the services provided by HUAWEI CLOUD or its own capabilities to ensure that the personal data is processed only for reasonable purposes and for purposes that the data subject has consented to. Customers can use <a href="#">Data Security Center(DSC)</a> provided by HUAWEI CLOUD to quickly identify personal data from their massive data and protect data accordingly. Customers can analyze personal data based on identified personal data to determine whether the collected personal data is necessary for business purposes, whether the data subjects have been informed of the purpose of data collection, and whether relevant personal data processing requirements have been met. In case of non-compliance, rectification measures can be taken in time to avoid illegal risks.

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Access and Correction	<ol style="list-style-type: none"> <li>Customers have the right to request access to their personal data. 1. Ensure that the personal data collected by the data controller is accurate and complete to ensure that all relevant and accurate personal data can be taken into account when personal data may be used to make decisions that affect individuals. data and to correct their personal data owned or controlled by a data controller.</li> <li>The request made by the customer to the data controller must be in writing and must include sufficient details to enable the data controller to judge: the applicant making the request; Personal data and use and disclosure of information requested by the applicant; Information such as personal data correction requests required by the applicant.</li> </ol>	<ol style="list-style-type: none"> <li>HUAWEI CLOUD has a dedicated team to communicate with customers. Customers can seek help from HUAWEI CLOUD through the service ticket service.</li> <li>Data subjects have privacy rights such as access rights, correction rights, deletion or restriction rights, portability rights, and consent withdrawal rights. Customers should develop a personal data management mechanism. Most HUAWEI CLOUD products or services provide data processing functions. Users can access, correct, delete, and export personal data.</li> </ol>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Accuracy	<ol style="list-style-type: none"> <li>1. Ensure that the personal data collected by the data controller is accurate and complete to ensure that all relevant and accurate personal data can be taken into account when personal data may be used to make decisions that affect individuals.</li> </ol>	<ol style="list-style-type: none"> <li>1. HUAWEI CLOUD provides multiple data security and privacy protection functions to ensure the accuracy of content data. For example, in the data storage phase, HUAWEI CLOUD provides data encryption (server-side encryption) for multiple services, such as Elastic Volume Service (EVS), Object Storage Service (OBS), Image Management Service (IMS), and Relational Database Service (RDS), and uses high-strength algorithms to encrypt stored data. In addition, the server-side encryption function integrates <a href="#">Data Encryption Workshop (DEW)</a>. Customers can use DEW to centrally manage keys throughout the lifecycle to ensure data integrity during storage.</li> <li>2. In the data use phase, customers can use <a href="#">Identity and Access Management (IAM)</a> provided by HUAWEI CLOUD to take enterprise-specific measures, such as user management, identity authentication, and fine-grained cloud resource access control, to prevent unauthorized modification of content data. During data transmission, customers can use multiple</li> </ol>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
		<p>encryption transmission mechanisms provided by HUAWEI CLOUD to ensure integrity during data transmission. For example, when customers provide website services over the Internet, they can use the certificate management service of HUAWEI CLOUD to implement trusted identity authentication and secure transmission based on encryption protocols. In hybrid cloud deployment and global deployment scenarios, you can use services such as <a href="#">Virtual Private Network (VPN)</a>, <a href="#">Direct Connect (DC)</a>, and <a href="#">Cloud Connect (CC)</a> provided by HUAWEI CLOUD.</p>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Protecting	<p>1. Before collecting, using, or disclosing personal data, the data controller shall make an assessment to ensure that the behavior will not adversely affect the individual. Protect personal data in its possession or control by making reasonable security plans to prevent unauthorized access to, collection, use, disclosure, copying, modification, disposal and loss or similar risks of the media or devices on which the personal data is stored.</p>	<p>1. Perform security configuration based on service and privacy protection requirements, such as operating system configuration, network settings, security protection, and database encryption policies, and set appropriate access control policies and password policies. In addition, customers can use multiple security services provided by HUAWEI CLOUD to meet their requirements of different security levels. For details, see <a href="#">HUAWEI CLOUD Security White Paper</a> and <a href="#">HUAWEI CLOUD Data Security White Paper</a> released by HUAWEI CLOUD.</p>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Retention Limits	<p>1. When the data controller is no longer able to meet the purpose for which personal data was collected and personal data is no longer required to be retained for legal or commercial purposes, stop retaining personal data or ensure that the data cannot identify individuals.</p>	<p>1. HUAWEI CLOUD does not touch customers' content data. Customers enjoy data autonomy. HUAWEI CLOUD provides multiple AZs for customers to select their own data storage regions.</p> <p>2. To meet the requirements for the purpose and period of data retention specified in laws and regulations, the customer shall formulate corresponding data retention policies and set the retention period with the help of related services provided by HUAWEI CLOUD. Personal data is deleted or anonymized when it is no longer required for legal or commercial purposes. Customers can use HUAWEI CLOUD services to anonymize sensitive personal data so that the data cannot be identified. For example, you can use <a href="#">Data Security Center(DSC)</a> to discover personal data stored in various databases, identify personal data based on rules, and hide personal data in real time based on anonymization policies. For customers' content data, users can customize the storage location and storage period on enabled nodes. HUAWEI CLOUD uses various data security</p>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
		technologies and related control measures, such as identity authentication and access control, data transmission and storage encryption, and log recording, to ensure the security of HUAWEI CLOUD services.

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Transfer Restriction	1. The data controller shall not transfer any personal data to a country or territory outside Singapore unless the protection of the transferred personal data complies with the data protection standards specified in the PDPA.	<p>1. When purchasing HUAWEI CLOUD products or services, customers must select AZs for storing content data and properly configure VPC policies based on their service compliance requirements. If personal data is stored on HUAWEI CLOUD, inform the data subject of the region where the personal data is stored. Matters relating to the cross-border transfer of data between the Customer and its individual users are defined as the responsibility of the Customer.</p> <p>2. The customer can specify the region where the content is stored. Without the customer's consent, HUAWEI CLOUD will not migrate the content from the selected region. In addition, customers can use the VPC service provided by HUAWEI CLOUD to set up a private network environment, divide network zones through subnet planning and routing policy configuration, and place storage in the internal subnet of the specified AZ.</p>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Leakage Notice	1. The data controller must assess in a reasonable and expeditious manner whether a data breach should be notified and, where assessed as notifiable, notify the affected individuals and/or the Commission.	<p>1. When a data breach occurs, the customer must assess in a reasonable and expeditious manner whether the data breach is a reportable data breach. Customer must notify the Commission and the affected individuals within 72 hours of the assessment of a data breach that results in significant harm to an individual or on a large scale. Submit to the Committee information such as the date and circumstances of the data breach, the control measures that have been taken, and the cause of the data breach; At the same time, notices should be sent to affected individuals, including information about the data breach, potential harm to individuals, control measures taken, and contact information of agents.</p> <p>2. HUAWEI CLOUD has developed a comprehensive personal data breach management system. Relevant personnel will analyze the impact of the incident according to the process. If the incident has affected or will affect cloud service customers, HUAWEI CLOUD will initiate a notification mechanism to notify the committee</p>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
		<p>and customers of the incident. The notification content includes but is not limited to the incident description, cause, impact, measures taken by HUAWEI CLOUD, and measures recommended by the customer. In addition, HUAWEI CLOUD has set up a 24/7 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations. In addition, the emergency plan and recovery process are executed to reduce the impact on services.</p>

Basic obligations of regulations	Requirements for HUAWEI CLOUD (as a personal data controller)	Measures Taken by HUAWEI CLOUD
Accountability obligations	1. Data controllers need to develop and implement the policies and practices necessary to implement PDPA obligations and make them known to the public. Specific requirements for this obligation include: Employees should be aware of such policies and practices; The data controller should establish a process for responding to complaints related to the Personal Data Protection Act, and the complaint method should be known to the public. The data controller shall have dedicated personnel responsible for PDPA compliance and publicizing relevant contact information.	1. Personal data contained in customer content is collected by the customer. If the customer chooses to use HUAWEI CLOUD services and stores the customer content containing personal data on HUAWEI CLOUD, the customer is responsible for establishing personal data protection policies and practices to ensure that the policies and practices comply with PDPA requirements. and make the data subject aware.  2. Customers can learn about HUAWEI CLOUD privacy protection information from the public documents of the Trust Center on the HUAWEI CLOUD official website. If necessary, customers can obtain HUAWEI CLOUD third-party audit reports to learn about HUAWEI CLOUD internal management and control.

## 5.2 HUAWEI CLOUD Products and Services Help Customers Implement Content Data Privacy and Security

HUAWEI CLOUD understands customers' privacy protection requirements and uses HUAWEI CLOUD products or services to help customers comply with Singapore privacy regulations based on their rich privacy protection practices and technical capabilities. The products and services provided by HUAWEI CLOUD cover network products, database products, security products, and management and deployment tools. The data protection, data deletion, network isolation, and permission

management functions of HUAWEI CLOUD help customers ensure content data privacy and security.

- **Management and Deployment Products**

Product	Description	Corresponding Core Requirements and Control Measures
<b>Identity and Access Management (IAM)</b>	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.  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.	Lawful Processing; Data Security;
<b>Cloud Trace Service (CTS)</b>	Customers can review logs to perform security analysis, review compliance, and locate issues, etc.  Customers can configure CTS object storage service to save operation records to CTS in real time and for a long period, protect the right to know of data owners, and enable quick searching.	Lawful Processing; Data Security; Rights of Data Subject;
<b>Cloud Eye Service (CES)</b>	Providing customers with a multidimensional monitoring platform for elastic cloud servers, bandwidth and other resources.  Through CES, 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.	Lawful Processing; Data Security;

Product	Description	Corresponding Core Requirements and Control Measures
<b>Log Tank Service</b> (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 owners' right to know.</p>	Lawful Processing; Rights of Data Subject;

- **Security Products**

Product	Description	Corresponding Core Requirements and Control Measures
<b>Database Security Service</b> (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>	Data Security;

<b>Data Encryption Workshop</b> (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>	Data Security;
<b>Web Application Firewall</b> (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>	Data Security;
<b>Vulnerability Scan Service</b> (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 integrity by automatically identifying security threats on their exposed websites or servers.</p>	Data Security;

<b>Advanced Anti-DDoS (AAD)</b>	<p>Advanced Anti-DDoS (AAD) is a value-added security defense service that defends against large volumetric DDoS attacks on Internet servers.</p> <p>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.</p>	Data Security;
<b>Data Security Center (DSC)</b>	<p>Data Security Center (DSC) is a new-generation cloud-native data security platform that provides basic data security capabilities which helps identify, classify, and mask sensitive or confidential data</p> <p>Customers can use DSC to integrate the status of each phase of the data security lifecycle to build a cloud service panorama to protect the security of data collection, storage, transmission, use, exchange, and destruction.</p>	Data Security;
<b>Cloud Certificate Manager (CCM)</b>	<p>Cloud Certificate Manager (CCM) is a cloud service that provides one-stop lifecycle management of digital certificates including SSL certificate and private certificate.</p> <p>Customers can use CCM to improve the confidentiality and security of SSL certificates and private certificates, improve the security of access and transmission channels, and reduce the risk of unauthorized data intrusion, access, or theft during transmission and access.</p>	Data Security;

- **Network Products**

Product	Description	Corresponding Core Requirements and Control Measures
<b>Virtual Private Network</b> (VPN)	<p>Virtual Private Network (VPN) establishes a flexible, scalable IPsec encrypted communication channel between customers' local data center and their VPC on HUAWEI CLOUD.</p> <p>Customers can build a flexible and scalable hybrid cloud computing environment, and improve their security posture with encryption of the communication channel.</p>	Data Security;
<b>Virtual Private Cloud</b> (VPC)	<p>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.</p> <p>VPC is the customer's private network on the cloud, with 100% isolation from other customers, enhancing the data security on the cloud.</p>	Data Security;

- **Storage Products**

Product	Description	Corresponding Core Requirements and Control Measures
<b>Volume Backup Service</b> (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>	Data Security;

Product	Description	Corresponding Core Requirements and Control Measures
<b>Cloud Server Backup Service</b> (CSBS)	Cloud Server Backup Service (CSBS) can simultaneously create a consistent online backup of multiple cloud drives within the cloud server.  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.	Data Security;

# 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, to be compliance with applicable laws and regulations.

HUAWEI CLOUD's capabilities and achievements in privacy protection and personal data security have been widely recognized worldwide. Up to now, HUAWEI CLOUD has obtained almost 20 domestic and foreign certifications from more than ten organizations, including global standard certifications related to privacy and data security and regional data security certifications.

## **Privacy Related Standard Certification:**

- **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 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.
- **SOC 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 SOC 1 Type II, SOC 2 Type II, SOC 2 Type I and released SOC 3 report.

**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
- ISO 27799 Health Information Security Management System Certification
- 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
- Management & Operations Stamp of Approval (M&O Program)
- NIST Cybersecurity Framework
- Payment Card Industry Three Domain Secure Certification (PCI 3DS)

**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 data security, and respects and protects customer privacy rights. HUAWEI CLOUD uses industry-wide 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 data 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 own situation when using cloud services and ensure compliance with the GDPR and other regulatory requirements when using HUAWEI CLOUD.

# 8

## Version History

---

Date	Version	Description
February 2023	3.0	Compliance Requirement Update
April 2022	2.0	Compliance Requirement Update
November 2019	1.0	First release