

White Paper for HUAWEI CLOUD Privacy Protection

Version V1.0
Date July 2019



HUAWEI TECHNOLOGIES CO., LTD.



Copyright © Huawei Technologies Co., Ltd. 2019. 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 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 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 Technologies Co., Ltd.

Address: Huawei Industrial Base

Bantian, Longgang

Shenzhen 518129

People's Republic of China

Website: Huawei – <https://www.huawei.com/en/>

<https://e.huawei.com/en/>

HUAWEI CLOUD – <https://www.huaweicloud.com/en-us/>

Email: support@huawei.com

Hotline: +86-4008-302-118



Introduction

With the continuous advances of cloud computing technologies and continuous evolution of cloud services, more and more enterprises choose to use public cloud services. In addition to bringing convenience to and extending the choices of enterprises, cloud services bring new opportunities and challenges. How to protect the security of personal data on cloud draws the focus and attention of countries, enterprises, and the public.

In November 2016, China issued the Cybersecurity Law of the People's Republic of China, which put forward a series of specific requirements for personal information protection. With the release of the Information Security Technology — Personal Information Security Specification and other specifications, China has increasingly strict requirements for personal information protection and regulation. In 2016, the EU issued the General Data Protection Regulation (GDPR), which officially came into effect in May 2018 and raised clear legal requirements for personal privacy rights. In recent years, countries including Argentina, New Zealand, Brazil, India, and Turkey have developed or amended their national privacy protection laws. The global situation of stricter privacy regulation poses higher requirements on privacy compliance.

HUAWEI CLOUD has made great efforts in privacy protection and achieved remarkable results. We hope that this white paper will share the privacy protection concepts and measures of HUAWEI CLOUD with customers and answer privacy protection questions that may arise during the use of HUAWEI CLOUD. Privacy protection is closely related to security; implementing privacy protection requires strong security capabilities. HUAWEI CLOUD has industry-leading experience and practice in terms of security. For details, see the HUAWEI CLOUD Security White Paper and White Paper for HUAWEI CLOUD Data Security.

HUAWEI CLOUD adheres to a neutral attitude, and safeguards strict service boundaries, ensuring that data is owned and used only by customers and creates value for customers. HUAWEI CLOUD commits to ensuring that related businesses comply with the privacy protection laws and regulations applicable to the countries/regions where the businesses are operated.

[HUAWEI CLOUD Security
White Paper and White
Paper for HUAWEI CLOUD
Data Security:
\[https://www.huaweicloud.
com/en-
us/securecenter/overallsaf
ety.html\]\(https://www.huaweicloud.com/en-us/securecenter/overallsecurity.html\)](https://www.huaweicloud.com/en-us/securecenter/overallsecurity.html)



Contents

- 1. Overview**
- 2. Privacy Protection Responsibilities**
- 3. HUAWEI CLOUD Privacy Protection System**
 - 3.1 Basic Privacy Protection Principles**
 - 3.2 Organization and Personnel Management
 - 3.3 Privacy Protection Process Framework
 - 3.4 Privacy Protection Management Tools
- 4. How HUAWEI CLOUD Protects Customers' Personal Data**
 - 4.1 Personal Data Lifecycle Management
 - 4.2 Security Technologies for Personal Data Protection
 - 4.3 Privacy Enhancing Technologies
- 5. How HUAWEI CLOUD Helps Customers Implement Personal Data Security**
 - 5.1 Privacy Management and Control in the Cloud Service Lifecycle
 - 5.2 Privacy Protection Service Capabilities
- 6. Privacy Protection Compliance and Certification**
- 7. Summary**

1. Overview

(1) Privacy: Defined broadly as "the right to be let alone." Physical privacy involves personal residence or property search, frisk, surveillance, or biometric information extraction. Information privacy refers to the ability of individuals to control, edit, manage, and delete their own information and determine how to communicate with others about this information. This white paper focuses on information privacy.

(2) Personal data: Personal data refers to any information relating to an identified or identifiable natural person ('data subject'). Personal data includes the natural person's email address, phone number, biometric feature (fingerprint), location data, IP address, medical record, religion, social insurance number, marital status, etc.



Cyber security and privacy⁽¹⁾ protection have always been vital to Huawei's survival. Since the establishment of Huawei, Huaweiers have been undertaking efforts in this direction. HUAWEI CLOUD has always fully understood the importance of privacy, inherits Huawei's over 30 years of practice and experience in privacy protection and over 20 years of practice and experience in more than 170 countries and regions, and has fully integrated cyber security and privacy protection into each cloud service, committing to **respecting and protecting customers' privacy and being a cloud partner with stable, reliable, secure, trustworthy, evolvable services for customers.**

HUAWEI CLOUD solemnly treats and actively takes the corresponding responsibilities and continues striving for this vision. As required by the company, HUAWEI CLOUD has **placed cyber security and privacy protection at top priorities.** On this basis, HUAWEI CLOUD sets up professional privacy protection teams, develops and optimizes processes, actively develops new technologies, and continuously builds HUAWEI CLOUD privacy protection capabilities.

The best practices of privacy protection depend on a comprehensive and systematic system: In compliance with global privacy protection laws and regulations, HUAWEI CLOUD has developed its own privacy protection system by referring to excellent practices widely recognized in the industry. HUAWEI CLOUD invests a large number of professionals and resources to support the research and application of new technologies and ensure the effective operation of the privacy protection system, ensuring that HUAWEI CLOUD is leading the industry in terms of privacy protection and achieving HUAWEI CLOUD's privacy protection objectives: **Safeguard strict service boundaries, protect customers' personal data security, and help customers implement privacy protection.**

This white paper provides an in-depth understanding of HUAWEI CLOUD's privacy protection system and describes how HUAWEI CLOUD protects personal data⁽²⁾ and helps customers implement personal data security.

2. Privacy Protection Responsibilities

As a cloud service provider (CSP), Huawei provides customers with various cloud services, such as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Implementing privacy and security in the complex cloud service environment requires the joint efforts of customers and HUAWEI CLOUD. Privacy protection poses clear requirements for enterprises. In this chapter, we will introduce the privacy protection responsibilities and obligations of customers in using cloud services based on the following responsibility model and how HUAWEI CLOUD helps you better implement privacy and security.

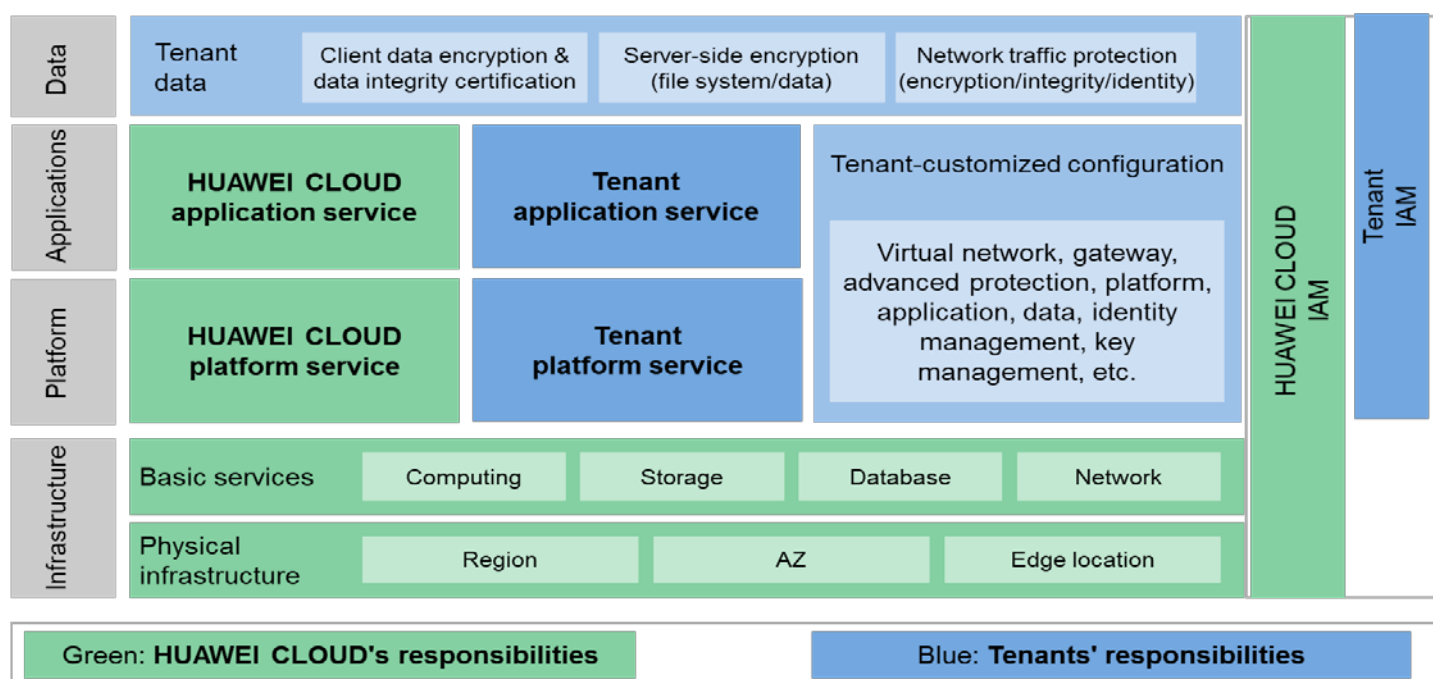


Figure 1: Privacy protection responsibility model

As shown in the above figure, HUAWEI CLOUD is responsible for the security and compliance of cloud services and provides customers with privacy features required for data processing, storage, and transfer. Regarding content data⁽³⁾, customers have all the rights and obligations, including privacy protection obligations. Customers shall develop security and privacy protection policies and measures to ensure personal data security and guarantee the rights of data subjects⁽⁴⁾ and the compliance of activities.

This model helps customers understand the privacy protection responsibilities and obligations of Huawei and customers. It also helps customers identify their personal data and develop appropriate personal data protection policies to better implement privacy protection.

(3) Content data: Content data refers to data stored or processed during the use of HUAWEI CLOUD services, including but not limited to documents, software, images, and audio and video files.

(4) Data subject: An identified or identifiable natural person.

According to the responsibility model, the major privacy protection responsibilities of HUAWEI CLOUD and customers are as follows:

Responsibilities of HUAWEI CLOUD:

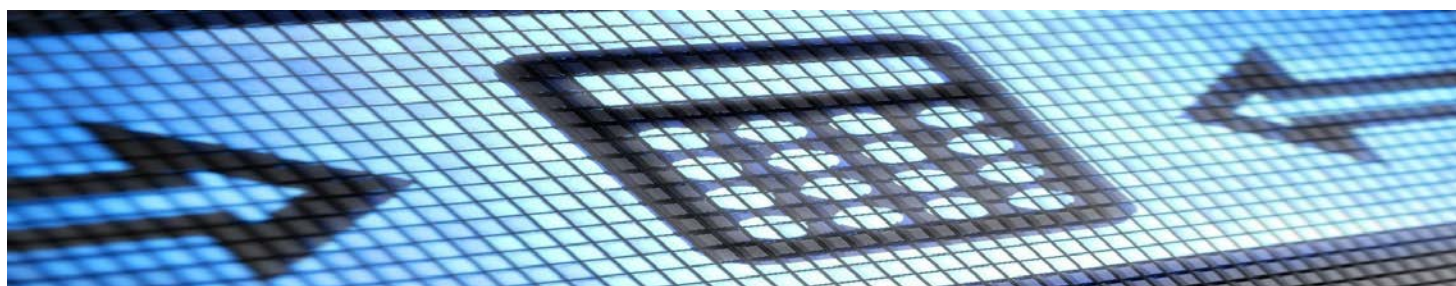
As a CSP, HUAWEI CLOUD provides a cloud platform consisting of the infrastructure, platform, and application layers, and is responsible for the security of the cloud platform infrastructure, such as the physical environment, software and hardware, computing, network, database, storage, platform layer, and application layer. The activities and cloud services of HUAWEI CLOUD comply with applicable privacy protection laws and regulations, providing customers with a stable, secure cloud environment that facilitates privacy protection.

HUAWEI CLOUD provides various privacy protection technologies for customers, including access control and identity authentication, data encryption, log and audit, and related privacy enhancing technologies (PETs). It also provides various cloud services by using these technologies, thereby helping customers protect privacy based on business requirements. HUAWEI CLOUD has a comprehensive privacy protection system and multi-dimensional management and control mechanisms for privacy protection, which enables the implementation of HUAWEI CLOUD's privacy protection responsibilities.

Responsibilities of customers:

Customers have full control over their content data. They shall correctly and comprehensively identify personal data on the cloud, select appropriate services, and develop security and privacy protection policies to protect personal data security. Customers shall also perform security configuration based on business and privacy protection requirements, such as operating system configuration, network settings, security protection, and database encryption policy configuration, and set appropriate access control policies and password policies. Customers can use multiple privacy protection services provided by HUAWEI CLOUD, for example, use data identification technology to identify and classify data, use access control service to set minimum permissions for personal data and assign permissions on demand, and use encryption to protect personal data storage and transfer.

A customer shall guarantee the rights of its data subjects and respond to data subjects' requests. When a personal data breach occurs, the customer shall notify the data subject and take corresponding measures. Customers can use multiple privacy protection services provided by HUAWEI CLOUD, for example, use the log function to retain the operation records of personal data, so as to ensure that users have the right to know their personal data. Customers shall ensure that personal data processing complies with applicable privacy protection laws and regulations. To help customers implement comprehensive privacy compliance, HUAWEI CLOUD provides multiple privacy protection services and compliance solutions.



3. HUAWEI CLOUD Privacy Protection System

(5) **Privacy by design:** Privacy by design (PbD) was first introduced as a methodology for privacy protection during product R&D. In recent years, it has gradually evolved into a management concept of privacy protection. PbD advocates **comprehensive, advanced, and proactive** integration of privacy protection into businesses and activities to help organizations take the initiative in privacy protection.

(6) **Privacy impact assessment:** Privacy impact assessment (PIA) is widely used and recognized as a common privacy assessment and design tool in the industry. PIA helps organizations identify and reduce privacy risks of businesses and identify and minimize potential privacy risks.

(7) **Privacy Statement:**
https://www.huaweicloud.com/en-us/declaration/sa_prp.html

HUAWEI CLOUD has established a comprehensive, standard, and unified privacy protection system to enable privacy protection of the cloud platform and help customers implement privacy protection. HUAWEI CLOUD develops seven privacy protection principles, uses the advanced concept of PbD⁽⁵⁾ that is recognized in the industry as a guideline, and generates its own privacy protection concept based on its actual situation. The privacy protection concept has been widely applied to various aspects of HUAWEI CLOUD, including organization and personnel management, personal data security management on the cloud platform, and privacy services provided to customers. In addition, HUAWEI CLOUD uses PIA⁽⁶⁾ to identify privacy risks and takes appropriate measures to eliminate or reduce risks. HUAWEI CLOUD respects users' privacy rights. It provides a clear Privacy Statement⁽⁷⁾ and customer feedback channels in prominent positions on the official website, helping customers understand the privacy protection information of HUAWEI CLOUD.

3.1 Basic Privacy Protection Principles



- **Lawfulness, fairness and transparency:** HUAWEI CLOUD processes personal data lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation:** HUAWEI CLOUD collects personal data for specified, explicit and legitimate 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 is anonymized or pseudonymized if possible, to reduce the risks for data subjects.

- **Accuracy:** HUAWEI CLOUD ensures that personal data is accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
- **Storage limitation:** Personal data is kept for no longer than is necessary for the purposes for which the personal data is processed.
- **Integrity and confidentiality:** Taking into account the existing technical capabilities, implementation cost, 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, and alteration or unauthorized access and disclosure, using appropriate technical or organizational measures.
- **Accountability:** HUAWEI CLOUD is responsible for and able to demonstrate compliance with the preceding principles.

3.2 Organization and Personnel Management

HUAWEI CLOUD has established a privacy protection organization, manages the organization and personnel based on the concept of PbD, and implements systematic privacy capability management for privacy protection personnel.

Privacy protection organization: HUAWEI CLOUD has set up a privacy protection expert team, including experts in the privacy protection field, legal affairs personnel, and dedicated cyber and information security personnel, to provide professional support for the privacy protection strategy and practice of HUAWEI CLOUD. In business teams of each product and service, HUAWEI CLOUD has set up dedicated privacy protection roles, who are responsible for privacy compliance and capability development of cloud services. In countries and regions where each business is located, HUAWEI CLOUD assigns dedicated legal and privacy protection personnel to help HUAWEI CLOUD implement local activities in compliance with applicable privacy laws and regulations.

Personnel management: HUAWEI CLOUD ensures that all employees' qualifications, capabilities, and behavior comply with privacy protection requirements and requires employees to pass privacy protection related appraisal every year.



In addition, HUAWEI CLOUD has identified privacy protection related positions and clearly defined the responsibilities of these positions. HUAWEI CLOUD also conducts background investigation and skill appraisal for new employees to ensure that they meet the requirements. All employees shall participate in the training on privacy protection awareness and pass the appraisal. When an employee is repositioned, HUAWEI CLOUD ensures that the original permissions are canceled.

Personnel skills: HUAWEI CLOUD regularly provides training in various forms on privacy protection awareness for all employees, so as to deepen employees' understanding of privacy protection and Huawei's privacy protection policies. Employees responsible for privacy protection are required to participate in skill training and pass the appraisal.

3.3 Privacy Protection Process Framework

HUAWEI CLOUD integrates the basic privacy protection principles into related processes and specifications to regulate privacy protection management of each work. HUAWEI CLOUD has established a comprehensive privacy protection process system and ensures that business activities comply with privacy protection requirements through a series of scientific and strict processes, such as privacy **process framework**, privacy protection policies, privacy protection design specifications, data subject rights assurance, storage limitation for personal data retention, and integrity and confidentiality.

3.4 Privacy Protection Management Tools

HUAWEI CLOUD uses multiple privacy protection platform tools to process privacy protection tasks more quickly, systematically, and efficiently. The **personal data auto-discovery tool** can detect whether a system or file contains personal data and identifies the types of personal data. This tool helps HUAWEI CLOUD take appropriate privacy protection measures. For example, if the personal data auto-discovery tool detects that a file contains personal data, HUAWEI CLOUD can encrypt the identified personal data or transfer the data via a secure channel. The **personal data management tool** can record the personal data types, storage locations, whether cross-border data transfer is involved, and personal data transfer in each HUAWEI CLOUD service scenario. By using this tool, HUAWEI CLOUD can manage the personal data in each service in a centralized manner, helping customers understand the types of personal data involved in services. The **PIA management tool** can record the list of personal data types and identify the reasons and purposes of personal data collection. The PIA management tool can also be used to analyze and assess privacy risks in related business scenarios, helping HUAWEI CLOUD identify privacy risks and develop and implement corresponding risk mitigation measures.



4. How HUAWEI CLOUD Protects Customers' Personal Data

HUAWEI CLOUD attaches great importance to customers' personal data security and adopts advanced and strict management and control mechanisms and technologies to ensure personal data security.

4.1 Personal Data Lifecycle Management

To better protect personal data and guarantee customers' data rights, HUAWEI CLOUD divides the personal data lifecycle into seven phases and implements privacy management and control throughout the lifecycle. HUAWEI CLOUD integrates the management and control requirements of each phase into all business processes.

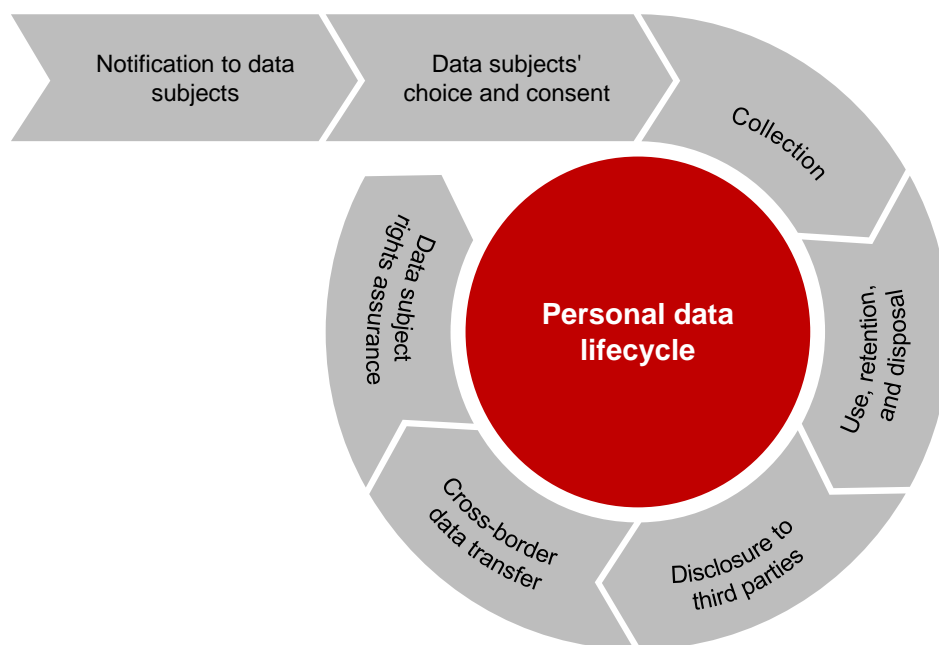


Figure 2: Personal data lifecycle

After obtaining a customer's consent, HUAWEI CLOUD collects the customer's personal data that is necessary for the provision of services and provides a privacy notice to inform the customer of the types of personal data to be collected, collection purposes, processing means, time limit, etc. For example, HUAWEI CLOUD provides a Privacy Statement and the mechanism for customers to give and withdraw consent on its official website. When personal data is to be collected in offline marketing activities, a privacy notice is provided at a prominent position, and a consent option is provided. HUAWEI CLOUD provides various configuration options on its official website. Customers can set the types of messages to be received and the means for receiving messages based on their preferences. For cloud services related to personal data processing, HUAWEI CLOUD informs customers of the types of personal data to be processed and the processing and storage means in the product documentation. Customers can take privacy protection measures accordingly.

HUAWEI CLOUD takes strict management and control measures on personal data stored on the HUAWEI CLOUD platform. To ensure personal data security, HUAWEI CLOUD manages personal data access, authentication, authorization, storage, and audit in a centralized manner. HUAWEI CLOUD specifies an explicit retention period. Personal data will be automatically deleted when the retention period expires. HUAWEI CLOUD implements role-based access permission management for O&M personnel. It grants permissions based on position requirements and regularly monitors the permissions to ensure that access permissions match position requirements. HUAWEI CLOUD regularly reviews and audits logs to check the rationality and necessity of personal data operations.

HUAWEI CLOUD conducts due diligence and privacy and security capability assessment for all suppliers as required. The privacy protection obligations and requirements of applicable laws and regulations for a supplier as a processor/sub-processor are specified in the contract to ensure that the supplier meets customers' privacy protection requirements. For other scenarios where HUAWEI CLOUD may disclose data to third parties in accordance with laws, see the Privacy Statement.

HUAWEI CLOUD has established data centers in multiple countries around the world. If cross-border data transfer is involved during operations and O&M, comply with local privacy protection laws and regulations and perform strict internal review. For example, cross-border data transfer shall be performed after a data transfer agreement is signed or the customer's explicit consent is obtained. This is to ensure that personal data is processed lawfully, fairly and in a transparent manner.

HUAWEI CLOUD has a professional team to respond to customers' personal data and privacy protection requests. After receiving a request from a customer, the team handles the request within the specified time and sends the handling result to the customer. HUAWEI CLOUD has set up a 24/7 professional security incident response team. This team informs customers of personal data breaches in compliance with applicable laws and regulations and executes the contingency plan and recovery process to reduce the impact on customers.

Data subject rights

assurance: Customers can send privacy protection requests to us via hws_security@huawei.com.

4.2 Security Technologies for Personal Data Protection

➤ For customers' personal data

Access control and identity authentication technologies are used to manage permissions for access to personal data. HUAWEI CLOUD defines and manages minimum access permissions based on role responsibilities. Employees have only the minimum permissions required, and the permissions will be deleted immediately when they are not required. HUAWEI CLOUD develops strict password policies and enables multi-factor authentication to strictly control permissions for access to personal data.

Encryption technologies are widely used to encrypt customers' personal data, ensuring the security of personal data during storage and transmission.

Logging and auditing technologies are used to record the access to and operations on key systems and the use of keys and regularly monitor and audit such access and operations to detect and correct inappropriate behavior in privacy protection in a timely manner. In addition, potential privacy protection and personal data security risks are analyzed so as to promptly respond to and address issues.

➤ For customers' content data

HUAWEI CLOUD uses various data security technologies and related management and control measures (such as identity authentication and access control, data transmission and storage encryption technologies, and logging) to ensure the security of HUAWEI CLOUD services and provides various security services to meet different security requirements of tenants. For details, see the *White Paper for HUAWEI CLOUD Data Security*.



4.3 Privacy Enhancing Technologies

The HUAWEI CLOUD research team is also committed to developing **PETs** to accumulate privacy protection engineering technical capabilities, so as to meet different privacy protection needs of customers. HUAWEI CLOUD already has a series of PETs, including equivalence class, differential privacy, anti-tracking, blockchain-based private payment, and privacy-preserving computation.

➤ Data masking

Data masking prevents the identification of user identities and sensitive information in data through various means, such as **masking, noise addition, enumeration, truncating, hashing, and tokenization**. This technology masks characters in personal data to protect data privacy and reduce data breach risks.

➤ Differential privacy

Differential privacy is a noise addition algorithm, which ensures a certain availability of data and prevents attackers from identifying the information of a specific user. Differential privacy injects noise to a database without knowing the content of the database. In this way, the dataset is fuzzed, but statistics are not affected. This technology reduces the probability of personal data being identified during database query.

➤ Searchable encryption

The searchable encryption technology can be used to search encrypted personal data, such as customers' email address, phone number, and ID card number, without plaintext display, which reduces personal data breach risks.



5. How HUAWEI CLOUD Helps Customers Implement Personal Data Security

HUAWEI CLOUD understands the significance of personal data protection to customers, and makes every effort to take management and control measures and provide services to help customers protect their personal data security.

5.1 Privacy Management and Control in the Cloud Service Lifecycle

To ensure that cloud services provided to customers meet compliance requirements and have privacy protection features, HUAWEI CLOUD puts privacy protection requirements at the top priority in each phase of the cloud service lifecycle based on the PbD concept. Strict privacy protection management and control requirements are imposed on each key node, to ensure and improve the privacy protection compliance of cloud services and ensure personal data security, thereby fully meeting customers' privacy protection requirements and helping customers protect the privacy of their users.

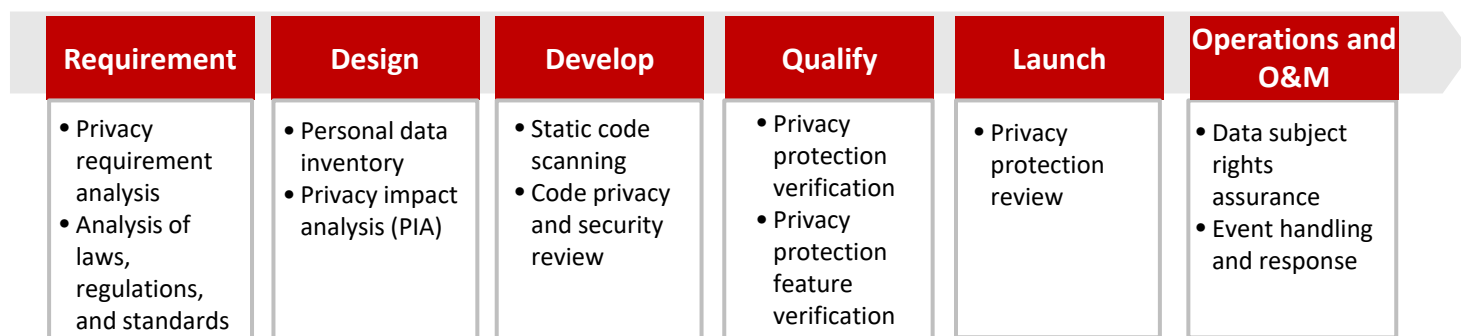


Figure 3: Privacy management and control in the cloud service lifecycle

Perform privacy protection management and control for HUAWEI CLOUD services throughout their lifecycle from requirement design to operations and O&M. Analyze privacy requirements and related laws and regulations during requirement analysis, and prioritize security and privacy requirements in service planning. In the design phase, sort out and record all personal data types involved, identify potential risks through PIA, and incorporate risk control measures into service design. In the development phase, perform static code scanning and privacy and security code review to ensure that the development process and code comply with Huawei's related development specifications. In the test phase, all privacy features must be strictly tested and reviewed by the expert team to ensure that privacy requirements and design are implemented in cloud services. The privacy compliance of cloud services is not limited to the R&D phase. During the continuous operations and O&M of cloud services, HUAWEI CLOUD uses various technical and management measures to prevent unauthorized access to and processing of personal data. This ensures the rights of data subjects and the continuous privacy and security of cloud services.



HUAWEI CLOUD provides various data security and privacy protection services. For more HUAWEI CLOUD services, go to <https://www.huaweicloud.com/en-us/product/>.

HUAWEI CLOUD takes privacy protection management and control measures throughout the lifecycle of each cloud service, so that:

- The PbD concept is implemented throughout the lifecycle to ensure that each cloud service meets privacy compliance requirements and has privacy protection features.
- Strict test and review are performed to ensure that privacy compliance requirements are implemented and privacy protection features are effective.
- Privacy protection does not end with product rollout. In the operations and O&M phase, HUAWEI CLOUD provides customers with compliant cloud services through the management and control of personnel and processes to help customers implement privacy protection.

5.2 Privacy Protection Service Capabilities

HUAWEI CLOUD integrates its technical experience and R&D achievements in new technologies into HUAWEI CLOUD services, providing customers with basic security and privacy protection services to help them protect personal data.

Identity and Access Management (IAM)

IAM enables HUAWEI CLOUD to provide customers with user management, identity authentication, and fine-grained cloud resource access control services applicable to enterprises.

Data Encryption Workshop (DEW)

DEW allows customers to encrypt personal data stored in databases and manage keys in a unified manner to enhance personal data security.

Monitoring , logging and auditing

HUAWEI CLOUD services provide the basic log recording function. Customers can configure this function through built-in functions of cloud services. In addition, HUAWEI CLOUD provides centralized and complete log recording and auditing services. Log Tank Service (LTS) and Cloud Trace Service (CTS).

Database Security Service (DBSS)

DBSS helps customers discover personal data and sensitive data stored in various databases and protect the data.

Data detection

It is the world's first structured data detection service. This service provides structured data detection and non-structured sensitive data detection. Users can quickly identify sensitive data from their huge volumes of data to meet GDPR and other compliance requirements. Non-compliant analysis reports can also be identified. This helps customers quickly build privacy compliance capabilities.

6. Privacy Protection Compliance and Certification

HUAWEI CLOUD complies with all local applicable privacy laws and regulations. HUAWEI CLOUD has a professional legal team, which closely monitors the update of laws and regulations, continuously tracks and analyzes global laws and regulations, and ensures compliance with laws and regulations.

HUAWEI CLOUD's capabilities and achievements in privacy protection and personal data security have been widely recognized by third-party certifications around the globe. Up to now, HUAWEI CLOUD has obtained certifications from more than 10 organizations in and outside China, including **ISO 27001, ISO 27018, ISO 27017, SOC2 (audit), PCI DSS Certification (for credit card data), CSA STAR Gold Certification, International Common Criteria (CC) EAL3+ Certification, Classified Cybersecurity Protection Level 3 (China), Trusted Cloud Service (TRUCS) (China), Certification for the Capability of Protecting Cloud Service User Data (China), MTCS Level 3 (Singapore)**, etc.

HUAWEI CLOUD actively focuses on the release of authoritative privacy certification mechanisms in the industry, and continuously raises higher requirements, optimizes its privacy protection system, and increases and updates security and privacy certifications. In addition, HUAWEI CLOUD works closely with privacy protection associations to explore cutting-edge privacy protection information and technologies to build its sustainable, secure privacy protection environment.



HUAWEI CLOUD shares compliance responsibilities with customers. Customers requiring compliance certifications can obtain necessary assistance from HUAWEI CLOUD. For HUAWEI CLOUD's certifications, visit the Trust Center:

<https://www.huaweicloud.com/en-us/securecenter/safetycompliance.html>



7. Summary

HUAWEI CLOUD business has been continuously growing in and outside China, facing more and higher requirements for providing intelligent, secure, and trustworthy cloud services to customers. HUAWEI CLOUD always adheres to Huawei's core value of "**staying customer-centric**", fully understands the importance of customers' personal data security, and respects and protects customers' privacy rights. HUAWEI CLOUD has industry-leading security and privacy protection technologies and provides cloud services and solutions to help customers cope with increasingly complex and open network environments and stricter privacy protection laws and regulations.

Placing cyber security and privacy protection at Huawei's top priorities, HUAWEI CLOUD will continue implementing the privacy protection vision and objectives in privacy protection practices, continuously increase investment, and continuously improve capabilities to provide customers with a secure and reliable cloud platform and privacy protection technologies to help customers protect personal data. HUAWEI CLOUD will always keep an open attitude, continuously research and study, and work with others to enhance and enrich HUAWEI CLOUD security and privacy protection services to help customers create value.

With the release of this white paper, HUAWEI CLOUD hopes to share our privacy protection practices and experience and continue working with customers to create a secure, trustworthy, and transparent cloud environment.

For more information about HUAWEI CLOUD privacy protection and related services, visit the HUAWEI CLOUD official website:

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

