White Paper for HUAWEI CLOUD Privacy Protection

Issue 2.0

Date 2021-01-22

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. 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

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: https://www.huawei.com

Email: support@huawei.com

Introduction

With the continuous advances of cloud computing technologies and cloud service evolution, an increasing number of enterprises choose to use cloud services, such as public cloud and hybrid cloud. Cloud provides a wide range of easy-to-use, cost-effective services, but also brings security challenges. Data security becomes a major concern for cloud service providers and enterprises that plan to migrate their services to cloud.

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. The release of the GDPR has a far-reaching impact worldwide, drawing people's attention to privacy protection. In recent years, countries including Argentina, New Zealand, Brazil, India, Turkey, and Thailand have released their national privacy protection laws. Privacy regulation is becoming strict all over the world and poses higher privacy compliance requirements for cloud service providers and international enterprises.

HUAWEI CLOUD is a brand of the ICT technologies, products, and solutions developed based on Huawei's more than 30 years of practices, providing customers with stable, secure, and ever-improving cloud services. HUAWEI CLOUD has made great efforts in privacy protection and achieved remarkable results. In this white paper, we hope to share with you the privacy protection concepts and measures of HUAWEI CLOUD, introduce how we protect customer data, and how the HUAWEI CLOUD services help customers protect privacy on the cloud.

 Copyright © Huawei Technologies Co., Ltd.

Contents

Introduction ii

1 Overview 1

2 Privacy Protection Compliance and Certification 3

2.1 Compliance 3

2.2 Standards and Certifications 4

3 Shared Responsibilities in Privacy Protection 6

3.1 HUAWEI CLOUD Responsibilities 7

3.2 Customer Responsibilities 7

4 How HUAWEI CLOUD Manages and Protects Data Privacy 9

4.1 Principles for Processing Personal Data 9

4.2 HUAWEI CLOUD Privacy Protection System 9

4.3 Technologies and Tools 12

5 How Customers Protects Privacy on the Cloud 15

5.1 Cloud Service Lifecycle Management Using DevSecOps 15

5.2 Privacy and Security Features of Cloud Services 16

5.3 Related Cloud Services 16

6 Summary 19

7 Change History 20

 Copyright © Huawei Technologies Co., Ltd.

1 Overview

Cyber security and privacy[1] protection have always been vital to Huawei's survival. Since the establishment of Huawei, we have been undertaking efforts towards this goal. HUAWEI CLOUD fully understands the importance of privacy, inherits Huawei's decades of practice and experience in privacy protection, and has fully integrated cyber security and privacy protection into each cloud service. Taking cyber security and privacy protection as Huawei's top priorities, HUAWEI CLOUD has determined its vision to respect and protect customer privacy, and to be a cloud partner that provides trustworthy, easy-to-use services. To achieve this vision, HUAWEI CLOUD set up professional privacy protection teams, and developed privacy protection processes and data security technologies, providing customers with stable, reliable, secure, trustworthy, and evolvable services.

HUAWEI CLOUD has developed a comprehensive privacy protection management system based on international privacy protection laws, regulations, and industry best practices. HUAWEI CLOUD invests a large number of professionals and resources to support the research and implementation of management measures and information technologies, facilitate the operations of the privacy protection system, and ensure the privacy protection compliance and sustainable development of HUAWEI CLOUD.

Privacy protection requires strong security capabilities. HUAWEI CLOUD has industry-leading practices and technical accumulations in cloud security. For details, see **HUAWEI CLOUD Security White Paper** and **HUAWEI CLOUD Data Security White Paper**.

HUAWEI CLOUD adheres to a neutral attitude and abides by service boundaries, ensuring that data is owned and used only by customers and creates value for customers. HUAWEI CLOUD is committed to complying with the privacy protection laws and regulations applicable to the countries/regions where it runs businesses.

——————————————————————

[1] Privacy: Broadly speaking, privacy is the right to be let alone. Physical privacy is infringed when an individual's personal residence or property is searched, the individual is frisked or monitored, or the individual's biometric information is extracted. Informational privacy is infringed when an individual is deprived of the rights to control, edit, manage, and delete their personal data and to decide how

 Copyright © Huawei Technologies Co., Ltd.

to communicate with others about his/her personal data. This white paper mainly talks about information privacy.

 Copyright © Huawei Technologies Co., Ltd.

2 Privacy Protection Compliance and Certification

2.1 Compliance

HUAWEI CLOUD complies with all applicable laws and regulations in regions where it runs its business. HUAWEI CLOUD has a professional legal team that tracks and analyzes the updates of laws and regulations applicable to HUAWEI CLOUD to ensure service compliance. HUAWEI CLOUD also developed compliance white papers to describe how its services comply with the laws, regulations, and industry regulatory requirements related to cyber security and privacy protection in certain countries and regions.

So far, HUAWEI CLOUD has released more than 10 compliance white papers in Trust Center[2]:

HUAWEI CLOUD Compliance with Brazil LGPD

HUAWEI CLOUD Compliance with Malaysia PDPA

HUAWEI CLOUD Compliance with Singapore PDPA

HUAWEI CLOUD Compliance with Thailand PDPA

 Copyright © Huawei Technologies Co., Ltd.

HUAWEI CLOUD Compliance with South Africa POPIA

HUAWEI CLOUD Compliance with PDPO of the Hong Kong Special Administrative Region of the People's Republic of China

HUAWEI CLOUD Compliance with HIPAA

HUAWEI CLOUD Practical Guide for PCI DSS

HUAWEI CLOUD Compliance with Singapore Financial Services Regulations & Guidelines

HUAWEI CLOUD Compliance with Hong Kong Financial Services Regulations & Guidelines

HUAWEI CLOUD User Guide to Financial Services Regulations & Guidelines in Thailand

2.2 Standards and Certifications

Huawei implements industry best practices in cyber security and privacy protection, and engages in the drafting and revision of related standards in international organizations such as Cloud Security Alliance (CSA) and International Association of Privacy Professionals (IAPP). HUAWEI CLOUD's cyber security and privacy protection capabilities and achievements have been widely recognized around the world. So far, HUAWEI CLOUD has earned certifications from more than 10 third-party organizations.

HUAWEI CLOUD's certifications[3] include:

ISO/IEC 27018:2014

ISO/IEC 29151:2017

ISO/IEC 27701:2019

BS 10012:2017

ISO/IEC 27799

PCI DSS certification

PCI 3DS certification

Trusted Cloud Service (TRUCS) - data protection capabilities of cloud service users (China)

SOC 2 Type I/II Report (privacy)

HUAWEI CLOUD follows the latest updates on authoritative privacy certification mechanisms in the industry, and continuously improves its privacy protection system to obtain and update security and privacy certifications. HUAWEI CLOUD also works closely with privacy protection associations to discuss the latest news and cutting-edge technologies, building a sustainable, secure, and trustworthy cloud platform environment.

——————————————————————

[2] HUAWEI CLOUD may add or update the privacy compliance white papers at any time. Information released on the HUAWEI CLOUD official website shall

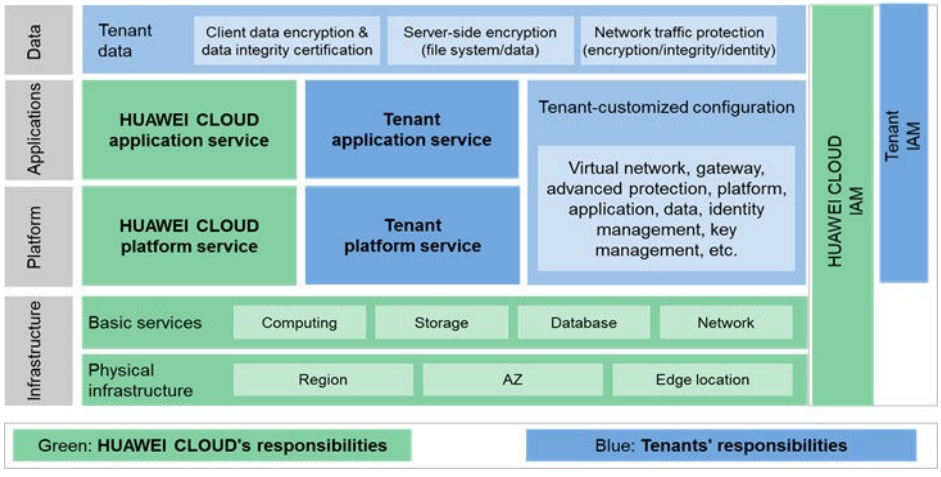
prevail. You can obtain the latest files from HUAWEI CLOUD Trust Center: **https://www.huaweicloud.com/intl/en-us/securecenter/resource.html**

[3] You can obtain copies of HUAWEI CLOUD certifications from HUAWEI CLOUD Trust Center: **https://www.huaweicloud.com/intl/en-us/securecenter/compliance.html**

3 Shared Responsibilities in Privacy Protection

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 customers' privacy protection responsibilities and obligations in using cloud services based on the following responsibility model and how HUAWEI CLOUD helps customers implement privacy and security.

Figure 3-1 HUAWEI CLOUD shared security responsibility model



As shown in this 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[4], 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[5] security and guarantee the rights of data subjects[6] and the compliance of activities.

 Copyright © Huawei Technologies Co., Ltd.

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 protect privacy.

Later sections will elaborate on the main privacy protection responsibilities of HUAWEI CLOUD and customers in the responsibility model.

3.1 HUAWEI CLOUD Responsibilities

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 infrastructure, such as the physical environment, hardware and software, compute, 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 a range of 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 developed a comprehensive privacy protection system and multi-dimensional management and control mechanisms for privacy protection to fulfill its responsibilities.

3.2 Customer Responsibilities

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 properly configure OS, network, security, database encryption policies, access control policies, and password policies based on business and privacy protection requirements. Customers can use multiple privacy protection services provided by HUAWEI CLOUD, for example, use data identification technologies to identify and classify data, use access control services to set minimum permissions for personal data and assign permissions on demand, and encrypt personal data to protect them during storage and transfer.

Customers shall guarantee the rights of its data subjects and respond to data subjects' requests. If a personal data breach occurs, customers shall notify the data subject and take corresponding measures. Customers can use multiple privacy protection services provided by HUAWEI CLOUD, for example, use the logging function to retain the operation records of personal data and ensure data subjects' right to know. 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.

————————————————————

[4] 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.

[5] Personal data or personal information refers to any information related to an identified or identifiable natural person ("Data Subject") who can be identified, directly or indirectly, in particular by reference to an identifier. Example: email address, telephone number, biometric information (such as a fingerprint), location data, IP address, health care information, religious belief, social security number, and marital status.

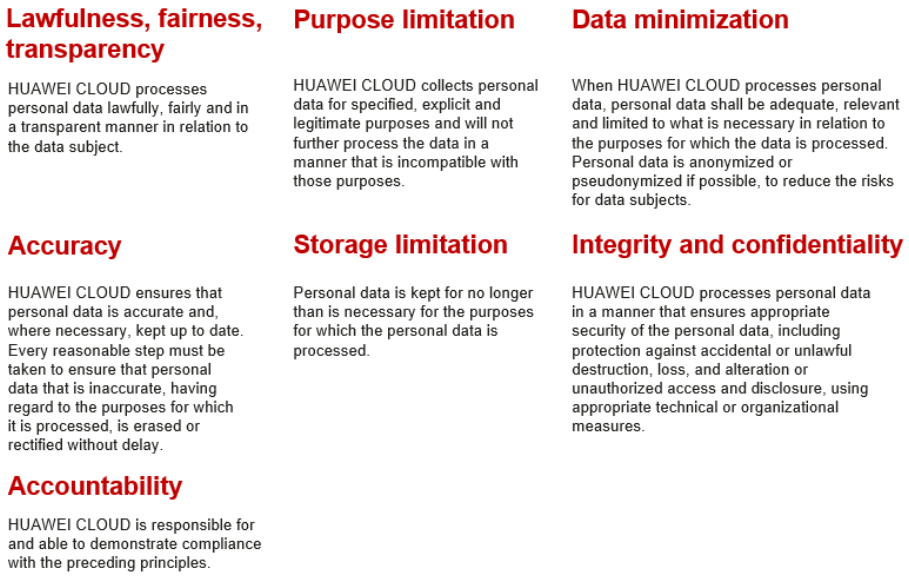
[6] Rights of data subjects include but are not limited to the right to know, right of access, right to data portability, and right to erasure (right to be forgotten).

 Copyright © Huawei Technologies Co., Ltd.

4 How HUAWEI CLOUD Manages and Protects Data Privacy

4.1 Principles for Processing Personal Data

In cloud service scenarios, we mainly discuss how we protect the rights of data subjects and the security of personal data. We have developed the following basic principles and have taken appropriate management and technical measures to ensure personal data processing comply with the principles.



4.2 HUAWEI CLOUD Privacy Protection System

HUAWEI CLOUD has established and keeps improving the privacy protection system for cloud services to protect customers' personal information and help customers protect user privacy on the cloud. The vision of HUAWEI CLOUD is to respect and protect customer privacy, and to be a cloud partner that provides trustworthy, easy-to-use services. HUAWEI CLOUD implements the idea of PbD [7],

Copyright © Huawei Technologies Co., Ltd.

protecting privacy in every design and activity. This section elaborates on HUAWEI CLOUD privacy protection in multiple respects.

Organization and Personnel Management

HUAWEI CLOUD has set up a dedicated privacy protection team and specified service owners to continuously improve privacy protection awareness and capabilities.

- **Privacy protection organization**

HUAWEI CLOUD has set up a privacy protection expert team consisting of experts in the privacy protection field, legal affairs personnel, and cyber and information security personnel, to provide professional support for the privacy protection strategy and practice of HUAWEI CLOUD. In each product and service team, 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 HUAWEI CLOUD runs its business, HUAWEI CLOUD assigns dedicated legal and privacy protection personnel to help 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 appraisal every year. HUAWEI CLOUD has sorted out positions related to privacy protection 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. When an employee is repositioned, HUAWEI CLOUD ensures that the employee's original permissions are canceled.

- **Awareness & capability improvement**

HUAWEI CLOUD regularly provides training in various forms 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 appraisals. Employees having the permissions for accessing customer network or processing data have to take part in certain privacy protection skill training and exams. All employees must successfully complete pre-job training and pass exams before assuming their roles.

Process Framework

HUAWEI CLOUD has widely applied the concept of PbD in its business domains and fully integrated basic privacy protection designs and technologies into business processes, implementing native privacy protection. HUAWEI CLOUD has established a comprehensive privacy protection process system, released privacy protection policies and objectives, released management regulations and process requirements to specify business specifications, and provided corresponding operation guides, tools, and templates to help employees carry out business activities in a compliant and efficient manner. All these ensure the implementation of basic privacy protection principles in HUAWEI CLOUD business activities, protecting personal data security and data subject rights.

Copyright © Huawei Technologies Co., Ltd.

Privacy Risk Management

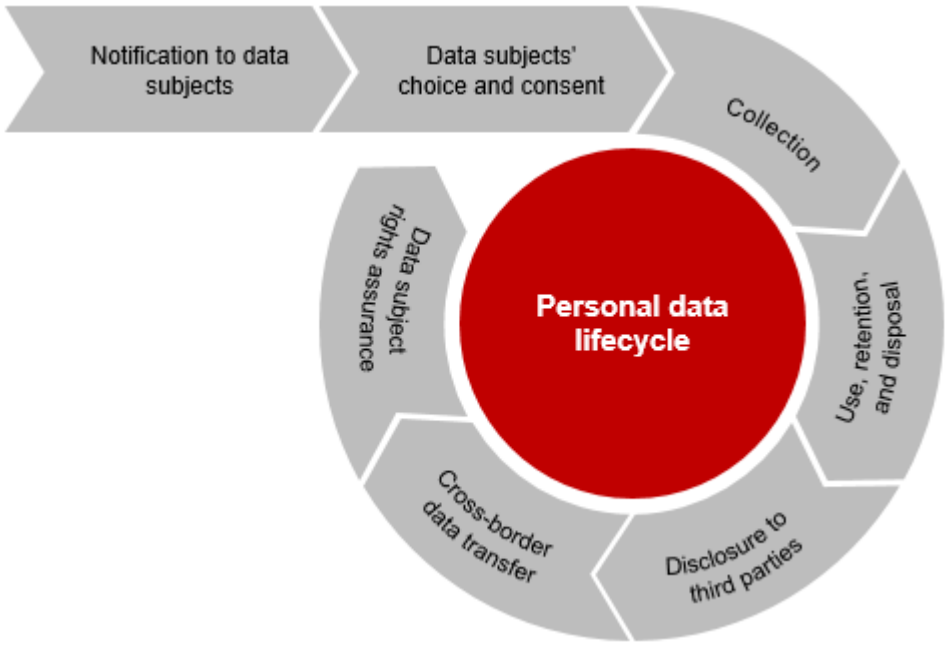
To effectively identify and control privacy risks, HUAWEI CLOUD carries out privacy risk analysis and management in every cloud service. HUAWEI CLOUD requires that privacy impact analysis (PIA) be performed before personal data is processed by a service. PIA identifies personal data items involved in services and data processing, possible compliance issues, impact on data subjects, and risks. PIA also provides risk control measures and plans. A business activity can start only if its privacy risks are reduced to an acceptable level.

For cloud services, HUAWEI CLOUD requires that PIA be carried out in the cloud service planning phase. Privacy risks must be analyzed in details, and all privacy risk control requirements must be met in design activities.

Personal Data Lifecycle Management

To better protect data subject rights and guarantee data security, HUAWEI CLOUD manages privacy throughout the service lifecycle, integrating the privacy assurance measures into each phase of its business process.

Figure 4-1 Personal data lifecycle



- **Notification, consent, and collection**

After obtaining a customer's consent, HUAWEI CLOUD collects the customer's personal data that is necessary for the provision of services and sends 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 also 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

Copyright © Huawei Technologies Co., Ltd.

preferences. For cloud services that involve personal data processing, HUAWEI CLOUD informs customers of the types of personal data to be processed and the means of processing and storage in the product documentation. Customers can take privacy protection measures accordingly.

- **Use, retention, and disposal**

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.

- **Disclosure to third parties**

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*.

- **Cross-border data transfer**

HUAWEI CLOUD has established data centers in multiple countries around the world. If cross-border data transfer is involved during service operations and O&M, the transfer shall comply with local privacy protection laws and regulations and pass 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.

- **Data subject rights assurance**

HUAWEI CLOUD has a professional team to respond to customers' personal data and privacy protection requests[8]. 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.

4.3 Technologies and Tools

HUAWEI CLOUD attaches great importance to the security of customers' personal data and adopts advanced, strict control mechanisms and technologies to protect it.

Copyright © Huawei Technologies Co., Ltd.

Technical Research and Application

Huawei keeps investing heavily in technology research and continuously applies new technologies to cyber security and privacy protection. For example, access control and identity authentication technologies are used to implement the principle of least privileges and precise data-level and operation-level management of system permissions. HUAWEI CLOUD encrypts customers' personal data to ensure its security during storage and transmission. Log and audit technologies are used to record the access to and operations on key systems and the use of keys. Periodic monitoring and audit are performed to detect and prevent suspicious privacy protection behavior in a timely manner. In addition, potential privacy protection and personal data security risks are analyzed to quickly respond to and fix problems. These technologies are integrated into HUAWEI CLOUD services to better protect personal data.

PETs

The HUAWEI CLOUD technical team is committed to developing Privacy Enhancement Technologies (PETs) and privacy protection engineering technical capabilities to meet diverse customer requirements. HUAWEI CLOUD PETs include equivalence class, differential privacy, anti-tracking, blockchain-based private payment, and privacy-preserving computation.

- **Data masking**

Data masking prevents disclosure of user identities and sensitive information by means of masking, noise addition, enumeration, truncating, hashing, and tokenization. This technology masks characters in personal data to protect privacy and reduce data breach risks.

- **Differential privacy**

Differential privacy is a noise addition algorithm, which ensures 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

Copyright © Huawei Technologies Co., Ltd.

database. In this way, the dataset is fuzzed, but statistics are not affected. This technology reduces the probability of personal data disclosure during database query.

- **Searchable encryption**

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

Tools

HUAWEI CLOUD uses multiple privacy protection tools to help HUAWEI CLOUD quickly, systematically, and efficiently manage privacy protection.

- **Data discovery and management**

The data discovery tool can identify personal data in systems, databases, or files, checking whether a business activity contains personal data and the type and transfer status of the data. The tool can also help users take appropriate privacy protection measures. (For details, see **DBSS** and DSC services.) Data Administration Service (DAS) helps HUAWEI CLOUD register and manage data assets throughout their lifecycle.

- **Privacy risk analysis**

The risk analysis process can be implemented using a range of tools, helping business teams identify privacy protection risks and develop and take countermeasures.

———————————————————

[7] PbD: 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.

[8] If you have any request regarding privacy issues, you can submit a **privacy request** or send an email to **privacy@huaweicloud.com**.

Copyright © Huawei Technologies Co., Ltd.

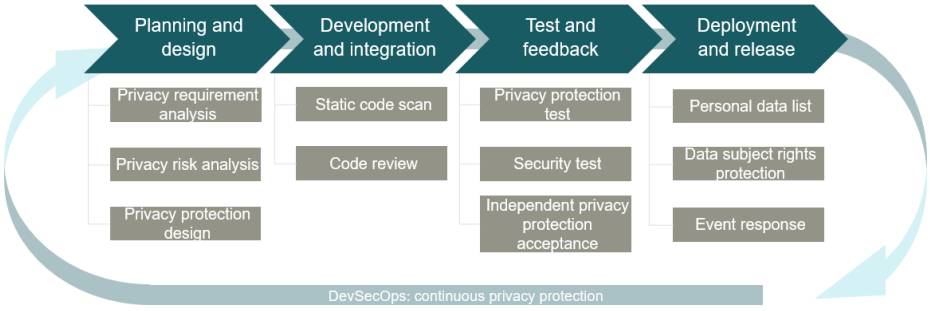
5 How Customers Protects Privacy on the Cloud

HUAWEI CLOUD has a deep understanding of the importance of personal data security and strives to take control measures and provide necessary services to help customers protect personal data. HUAWEI CLOUD uses various data security technologies and control measures, such as identity authentication and access control, data transmission and storage encryption, and logging, to ensure the security of HUAWEI CLOUD services. HUAWEI CLOUD also provides various security services to meet tenants' requirements. For details, see the *HUAWEI CLOUD Data Security White Paper*.

5.1 Cloud Service Lifecycle Management Using DevSecOps

HUAWEI CLOUD understands that IaaS, PaaS, and SaaS services must be secure enough to lay a solid foundation for privacy assurance. During R&D, to ensure cloud services are protected with default privacy protection features throughout their lifecycles, HUAWEI CLOUD integrates security and privacy protection measures into DevOps phases to develop a process named DevSecOps. HUAWEI CLOUD also sets strict privacy protection requirements and takes control measures to ensure cloud services are capable of protecting personal data and fully meet customers' privacy protection requirements. The following figure illustrates the major privacy protection control points in a cloud service lifecycle.

Figure 5-1 Cloud service lifecycle and privacy control



The DevSecOps process has the following advantages:

- The PbD concept is implemented throughout the lifecycle to ensure every cloud service meets privacy compliance requirements and has privacy protection features.
- Strict tests and reviews verify that privacy compliance requirements are met and privacy protection features are effective.
- Privacy protection continues after product rollout. In the O&M phase, HUAWEI CLOUD ensures service compliance by personnel and process management, helping customers protect privacy.

5.2 Privacy and Security Features of Cloud Services

HUAWEI CLOUD ensures all HUAWEI CLOUD services have default security and privacy features by implementing strict R&D process control measures, including:

- **Privacy notice**

For cloud services involving personal data processing, HUAWEI CLOUD provides a personal data list and describes the service scenarios, purposes, data scope, and processing methods in the cloud service documentation, helping customers evaluate compliance risks and privacy control measures of the service. In certain cloud services, customers can configure privacy notifications based on service compliance requirements.

- **Encryption**

By default, cloud services encrypt customers' sensitive personal data (if any) and all data transmitted over untrusted networks. Certain cloud services allow customers to configure whether and how to encrypt data. HUAWEI CLOUD also provides encryption management services.

- **Permission control**

Access control and permission management are essential for privacy protection. All cloud services are required to integrate Identity and Access Management (IAM) and to verify user identities and permissions.

- **Log audit**

Traceability is a basic principle of HUAWEI CLOUD privacy protection. Logging is a basic feature of HUAWEI CLOUD services. Customers can use Cloud Trace Service (CTS) or the logging function of other cloud services to support audit logs and meet compliance requirements.

For details about HUAWEI CLOUD security and privacy protection features, including data minimization, consent and consent withdrawal, and data retention, visit **the HUAWEI CLOUD website**.

5.3 Related Cloud Services

In addition to the privacy features described in the previous sections, HUAWEI CLOUD also provides comprehensive privacy protection solutions and a wide range of cloud services to help customers develop and improve security and privacy

protection capabilities on the cloud. Customers can choose services as needed to manage and protect personal data.

IAM

Identity and Access Management (IAM) can authenticate users, assign permissions, and manage employee, system, and application accounts. Customers can allow certain users to access certain resources.

DEW

Data Encryption Workshop (DEW) is a comprehensive cloud data encryption service. It provides Key Management Service (KMS), Key Pair Service (KPS), and Dedicated Hardware Security Module (Dedicated HSM). HSMs can protect the security of your keys, and can be integrated with other HUAWEI CLOUD services. Additionally, DEW enables customers to develop customized encryption applications.

DBSS

Database Security Service (DBSS) protects databases on the cloud. Taking advantage of its reverse proxy and machine learning technologies, it detects and masks sensitive data, audits databases, and defends against injection attacks.

LTS

Log Tank Service (LTS) aggregates, quickly searches for, and dumps logs; use charts to illustrate statistics; and provides massive storage and structured processing capabilities. All these facilitate O&M, network log analysis, compliance assurance, and operations analysis.

CTS

Cloud Trace Service (CTS) records operations on cloud resources under customer accounts. Based on the records, customers can perform security analysis, track resource changes, conduct compliance audits, and locate faults. To store operation records for a long time, customers can subscribe to Object Storage Service (OBS) and synchronize operation records to OBS in real time.

For more HUAWEI CLOUD services, visit the following website:

https://www.huaweicloud.com/intl/en-us/product/

6 Summary

HUAWEI CLOUD business has been continuously growing in and outside China, facing more and higher requirements for 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 network environment and stricter privacy protection laws and regulations.

Taking cyber security and privacy protection as Huawei's top priorities, HUAWEI CLOUD will continue implementing the privacy protection vision and objectives in privacy protection practices to provide customers with secure, reliable cloud services to protect personal data. HUAWEI CLOUD embraces new technologies and collaborates with partners, continuously improving security and privacy protection services and capabilities. HUAWEI CLOUD helps customers create value, meanwhile working with customers to protect personal privacy on the cloud.

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

For more information, visit the HUAWEI CLOUD website:

https://www.huaweicloud.com/intl/en-us/

 Copyright © Huawei Technologies Co., Ltd.

7 Change History

Date	Version	Description
July 2019	1.0	This is the first official release.
January 2021	2.0	Routine update

 Copyright © Huawei Technologies Co., Ltd.