HUAWEI CLOUD Compliance Instruction with PDPL of the Republic of Peru

Issue 2.0

Date 2025-05-07

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Overview

1.1 Scope of Application

The information provided in this document applies to HUAWEI CLOUD and all its products and services available in the Republic of Peru.

1.2 Purpose of Publication

This document is intended to help customers understand:

1. HUAWEI CLOUD's privacy protection shared responsibility model;
2. Peruvian privacy protection laws and regulations;
3. Based on the responsibility model, how HUAWEI CLOUD complies with Peruvian privacy protection laws and regulations;
4. Based on the liability model, customers may need to comply with Peruvian privacy protection laws and regulations;
5. How HUAWEI CLOUD helps customers meet privacy compliance requirements.

2 Personal Data Processed by HUAWEI CLOUD

When providing services to customers, HUAWEI CLOUD usually processes the following two types of personal data:

- **Account data**:

  Account data refers to the personal data provided by customers to HUAWEI CLOUD for service purposes during interaction with HUAWEI CLOUD, and related to customer account creation or management. For example, the user name, mobile phone number, and email address provided by the customer to HUAWEI CLOUD when creating an account. Name, detailed address, postal code, and mobile number of the recipient provided by the customer to HUAWEI CLOUD when the customer uses the address management service.

  The practices described in HUAWEI CLOUD Privacy Policy Statement are applicable to account data. HUAWEI CLOUD will process account data in accordance with the Privacy Policy Statement, such as collecting, storing, and using account data in accordance with the data minimization principle, and taking appropriate technical and organizational measures to protect account data security.

- **Customer data:**

  Customer data refers to the personal data contained in customer content.

  Customer Content refers to all data, software, text, images, videos, and audio, etc. stored and processed by the customer and/or the customer's end users on HUAWEI CLOUD in any format, as well as the calculation results generated by the service.

  Customer owns and can control customer content (including customer data):

  1) The customer can choose which HUAWEI CLOUD services to process the customer's content.

  2) Customers can choose where their content is stored.

  3) Customers can choose how to protect their content.

  4) The customer can manage and control access to the customer's content.

The practices described in Huawei Cloud Data Processing Addendum are applicable to customer data. HUAWEI CLOUD will process customer data in accordance with the Data Processing Addendum, including processing customer data only according to customer instructions and taking security measures to protect customer data.

3 HUAWEI CLOUD Shared Responsibility Model

Ensuring the security and compliance of your cloud services is a responsibility shared between you and Huawei Cloud. Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. Cloud security cannot be guaranteed by a single party alone. It requires the combined efforts of both you and Huawei Cloud to ensure a secure environment.

Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. You can select from the different cloud service categories, such as IaaS, PaaS, and SaaS, shown in the figure, to meet different service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

When privacy protection requirements may apply to customer content, the Shared Responsibility Model helps HUAWEI CLOUD and the customer understand their respective roles and responsibilities.

Figure 3-1 Shared Responsibility Model

Huawei Cloud's responsibilities: Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.

Customer responsibilities: As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.

In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the middleware, database, and network access under their control.

In SaaS scenario, customers have control over their own content, accounts, and permissions. They are responsible for ensuring legal compliance, securing their content, and configuring and protecting their accounts and permissions.

4 Overview of Peruvian Personal Data Protection Law (PDPL)

4.1 Background of Regulations

In 1993, the Peruvian Constitution recognized the protection of personal data as a fundamental right, providing a constitutional basis for the protection of personal data security.

In 2011, Peru promulgated Law No.29733 on the Protection of Personal Data (PDPL), which establishes a systematic and comprehensive mechanism for the protection of personal data. This law is currently the most important legal basis in Peru for the protection of the security of personal data.

Since then, the PDPL has been revised several times in order to further improve its operability. In 2013, Peru promulgated Supreme Decree No. 003-2013-JUS (Supreme Decree No.003-2013-JUS). This decree details the contents of the PDPL, makes the responsibilities of all parties involved in the protection of personal data clearer, and promotes the smooth implementation of the PDPL.

In 2017, Peru issued Legislative Decree No. 1353, which revised and updated the PDPL again, adding new content such as the situations in which personal data is processed without the consent of the personal data subject, so that it can better adapt to social development.

In 2024, Supreme Decree No. 016-2024-JUS was published in the Official Gazette of Peru, approving the revision of Law Regulation No. 29733, introducing key changes and repealing the previous version.

This document applies only to the provisions of the PDPL Regulations and related decrees in force at the date of publication and may be adjusted accordingly in accordance with applicable laws and regulations.

4.2 Role Division

The PDPL in Peru defines three key roles: data subject, data controller, and data processor.

Data Subject: Individuals whose personal data is processed.

Data controller: a natural person, a legal entity governed by private law, or a public entity that decides the purpose and manner of processing personal data. This definition is not limited to the owner of the database, but also includes anyone who decides to process personal data, even if not in the personal database.

Data processor: a natural person, legal entity governed by private law, or public entity that processes data on behalf of the controller or holder of a personal database or whose orders it orders.

5 How HUAWEI CLOUD Complies with the Requirements of Peruvian PDPL

5.1 HUAWEI CLOUD's Role under Peruvian PDPL

Personal data processed by HUAWEI CLOUD includes account data and customer data.

- HUAWEI CLOUD acts as the controller of account data

During the interaction between the customer and HUAWEI CLOUD, the customer submits account data to HUAWEI CLOUD. HUAWEI CLOUD determines the collection method and processing purpose of the account data. Therefore, HUAWEI CLOUD acts as the data controller. HUAWEI CLOUD will also be responsible for the security and privacy protection of the customer's personal data based on the privacy laws of the Peru, ensure that the collection, processing, storage, and transmission of personal data comply with laws and regulations, and respond to personal data subject rights requests.

- HUAWEI CLOUD acts as the processor of customer data

The customer owns and fully controls customer data. The customer selects and uses HUAWEI CLOUD services to store and process customer data. The customer provides instructions through function configuration or APIs provided by the cloud service. HUAWEI CLOUD processes data based on the instructions provided by the customer. When the customer is the data controller, HUAWEI CLOUD acts as a data processor for customers. If the customer is a data processor, HUAWEI CLOUD acts as a sub-processor.

5.2 How HUAWEI CLOUD Complies with PDPL Requirements as a Data Controller

Huawei Cloud integrates cyber security and privacy protection into cloud services, and promises to respect and protect customer privacy while providing customers with stable, reliable, secure, trustworthy, and sustainable services.

HUAWEI CLOUD takes its responsibilities seriously and complies with global privacy protection laws and regulations. HUAWEI CLOUD establishes a professional privacy protection team, establishes and optimizes processes, actively develops new technologies, and continuously builds privacy protection capabilities to achieve the privacy protection objective of HUAWEI CLOUD: Comply with strict service boundaries to protect customers' personal data security and help customers achieve privacy protection.

5.2.1 HUAWEI CLOUD Basic Privacy Protection Principles

HUAWEI CLOUD considers privacy in design based on the PbD principle, that is, protecting personal data through design and applying the concept of personal data protection to each phase of products and services through technical means. HUAWEI CLOUD implements the following 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**

Considering 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.

5.2.2 How HUAWEI CLOUD Complies with PDPL Requirements

According to the privacy laws of Peru, HUAWEI CLOUD proactively takes measures to fulfill the legal obligations of data controllers. The following describes the specific requirements of Peru privacy laws applicable to HUAWEI CLOUD and the supplementary description of the corresponding measures taken by HUAWEI CLOUD.

Basic obligations of regulations	Requirements for HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
Notice and Consent	Follow the principles of legality, legitimacy, and necessity. When processing personal information	1. When a customer registers an account, HUAWEI CLOUD displays the Privacy Policy

Basic obligations of regulations	Requirements for HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
PDPL Article 5. Principle of consent PDPL Directive: Article 1. Consent to the processing of personal data Article 2-6: Characteristics of valid consent Article 13: Conditions for Transfer of Personal Data	based on personal consent, comply with relevant regulations, such as not collecting information beyond the scope or obtaining consent by misleading means. Before processing personal information, the individual shall be clearly informed of the processor's information, purpose, method, type, and retention period. Individual consent must be obtained for scenarios such as processing sensitive personal information and providing personal information to third parties. When the purpose, method, or type of processing is changed, the consent must be obtained again.	Statement to the customer, clearly notifies the customer of the types of personal data to be collected, the purpose and legal basis of personal data collection and processing, personal data disclosure to third parties, and data subjects' rights, completely identifies himself as Data Controller in the terms of point (d) in left column and obtains the customer's consent. If the scope or purpose of personal data collected by HUAWEI CLOUD changes, the Privacy Policy Statement will be updated and the customer's consent will be obtained again. 2. If the personal data items collected or processing purposes of a service are inconsistent with those in the Privacy Policy Statement, the service will provide an independent service statement to inform customers of the collected personal data items and processing purposes and obtain customers' consent in the terms of column on the left. 3. HUAWEI CLOUD informs customers of the right to withdraw their consent to their personal data at any time in the Privacy Policy Statement. HUAWEI CLOUD provides customers with an easy-to-use consent withdrawal channel. Customers have the right to decide whether and when to withdraw their consent to stop the collection of their personal data by HUAWEI CLOUD products or services. However, the customer's decision to withdraw the consent or authorization will not affect the personal data processing that has been

Basic obligations of regulations	Requirements for HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
		performed based on the customer's authorization. 4. HUAWEI CLOUD explicitly informs customers of the legal basis for processing their personal data in the Privacy Policy Statement. HUAWEI CLOUD processes customers' personal data based on one or more of the following legal bases: a) Customer’s consent; b) To enter into a contract with, or to fulfill contractual obligations to, the customer or the legal entity on whose behalf the customer is acting, such as providing services, responding to customer requests, or providing customer support; c) Necessary for our legitimate interests or those of a third party; d) Necessary to comply with applicable laws and legal obligations.
Purpose Limitation PDPL: Article 6. Principle of purpose Article 7. Principle of proportionality Article 13. Scope of the processing of personal data PDPL Directive: Article 26: Processing of data for advertising and commercial prospecting	Personal data must be collected for specific, clear, and legitimate purposes. The processing must respect the rights of data subjects and comply with the principle of proportionality. That is, the processing method must be appropriate for the purpose and not excessive. Data subjects' consent is required when personal data is processed for advertising and commercial promotion. No further contact or data processing shall be allowed without consent after the first contact.	1. HUAWEI CLOUD only collects personal data necessary for service processing. The Privacy Policy Statement clearly informs HUAWEI CLOUD how to collect, use, and disclose customers' personal data, including the scenarios of collecting personal data, types of personal data, purposes of using personal data, and scenarios of disclosing personal data to third parties. Disclosed personal data types, etc. 2.The personal data collected, used, and disclosed by HUAWEI CLOUD is limited to the content specified in the Privacy Policy Statement. If the collection, use, and disclosure of personal data are changed, HUAWEI CLOUD

Basic obligations of regulations	Requirements for HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
		will notify customers of the changes by updating the Privacy Policy Statement. If the legal basis for personal data processing is the customer's consent, HUAWEI CLOUD will obtain the customer's consent again.
Data subject rights PDPL: Article 18-27 PDPL Directive: Article 63-87 Right of information\Right of access\ Right to update, inclusion, rectification and erasure\ Right to prevent the provision\ Right to object\ Right to objective processing	During the processing of personal data, the rights of data subjects shall be fully and effectively guaranteed. Right to know and access: Data subjects have the right to obtain all relevant information through access. Data portability: Where processing is based on consent or contract and is conducted by automated means, data subjects may request that their personal data be transmitted to other data controllers or responsible persons in a structured, common and machine-readable format. Right of correction, right of deletion or cancellation, right of objection: Data subjects have the right to request correction of inaccurate data; may request deletion or cancellation of data when the data is no longer necessary, when the processing period expires, when consent is withdrawn, etc.; The processing of their personal data can be opposed at any time, and the enterprise needs to stop the processing. Right to process data objectively: Data subjects have the right not to be involved in automated decisions that have significant impact.	1. Section 7 in the Privacy Policy Statement of HUAWEI CLOUD has informed customers of how to access and correct their personal data. That is, customers can visit the HUAWEI CLOUD website and log into the account center to access and correct their personal data. 2. In addition to access and correction, section 7 of the HUAWEI CLOUD Privacy Policy Statement also informs data subjects of their rights to deletion, objection, restriction, portability, and complaint to the supervisory authority. If the customer needs assistance from HUAWEI CLOUD in exercising data subjects' rights, the customer can contact HUAWEI CLOUD through the data subject rights portal or email provided in section 11 of the HUAWEI CLOUD Privacy Policy Statement.
Accuracy PDPL: Principle of quality	The personal data processed must be true, accurate and as up-to-date, necessary, relevant and sufficient as possible for the purposes for which the data were collected.	HUAWEI CLOUD takes different measures to ensure the accuracy of customer account data. For example, HUAWEI CLOUD verifies the validity of personal data entered by customers to enhance the standardization and accuracy of

Basic obligations of regulations	Requirements for HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
		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.
Protecting PDPL: Article 9. Principle of security Article 16. Security of personal data processing Article 17. Confidentiality of personal data PDPL Directive: TITLE I PROCESSING OF PERSONAL DATA CHAPTER VI SECURITY MEASURE	Keep personal data under secure conditions to prevent it from being tampered with, lost, accessed, and used without authorization. Security assurance measures: Take necessary technical, organizational, and legal measures to ensure the security of personal data and prevent data from being tampered with, lost, processed, or accessed without authorization. Security measures shall be appropriate to the processing activity and the type of data. Data backup and recovery: Design and implement security control measures, including maintaining security areas, protecting devices, and ensuring that security backups are generated and verified. Backups are performed at least weekly unless the data is not updated and security measures are required for storage, transfer, and destruction. You need to verify the integrity of the backup data and restore the data in case of interruption or damage. Data transmission security: The exchange of personal data from the processing or storage environment to any destination outside the entity must be authorized by the data subject, using the means of transportation authorized by the data subject, and taking measures such as encryption, digital signature, and certificate to prevent unauthorized access, loss, or	HUAWEI CLOUD takes the following measures to protect account data from unauthorized access, modification, and disclosure: a) Set up a privacy protection organization to identify and manage personal data protection risks. b) Develop data security and personal data protection policies, including security vulnerability response and personal data breach management processes, to reduce privacy security risks caused by personal data breaches and guide relevant departments to process personal data in compliance with laws and regulations. c) Organize security and privacy protection training courses, tests, and publicize activities to improve employees' personal data protection awareness. d) take reasonable and practicable steps to ensure that the personal data collected are kept to a minimum and are relevant for the purposes for which they are processed. e) Implement a series of measures, such as entrance and exit control, access control system, and closed-circuit television (CCTV) system to ensure the physical security of data centers and prevent unauthorized access, damage, or interference to HUAWEI CLOUD infrastructure. f) Deploy access control

Basic obligations of regulations	Requirements for HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
	damage. Non-automated document storage: Facilities such as cabinets storing non-automated documents shall be protected by keys or other equivalent devices, data storage areas shall be closed when not necessary, keys or openers shall be formally assigned, and transfer and allocation procedures shall be in place. Document copying and destruction: Documents containing personal data must be generated or copied under the control of authorized personnel. Discarded copies must be destroyed to prevent information access or subsequent recovery. Document access control: Document access is restricted to authorized personnel. A mechanism must be established to identify access to documents of multiple users. Access to documents by unauthorized personnel must be properly recorded. Non-automated document transfer: When transferring non-automated documents, take measures to prevent unauthorized access, misuse, manipulation, and modification of data.	mechanisms to authenticate personnel's access to data and implement hierarchical permission management based on service requirements and personnel levels, ensuring that only authorized personnel can access personal data. g) Clearly define and assign cybersecurity roles and responsibilities, implement segregation of duties based on risk assessments, mitigate risks, and protect data processing systems from unauthorized use. h) Encrypt and pseudonymize personal data using recommended industry standard protocols, as appropriate, during data storage and transmission to prevent data breaches and unauthorized access. i) Degauss the discarded storage media before returning them to the warehouse to ensure that the media are overwritten by software before being discarded to prevent data leakage. In cases where this is not possible (CDs, DVDs, etc.), physical destruction will take place. j) implement appropriate operational security management and technical measures, including identity authentication and access control, change and event management, vulnerability management, configuration management, event logging, continuous monitoring of cybersecurity incidents and threats, timely detection of anomalies, and proactive measures to deal with them; ensure that personal data is not read, copied, altered or deleted by unauthorized persons. k) Deploy protection mechanisms such as anti-DDoS systems and intrusion detection systems to protect network from

Basic obligations of regulations	Requirements for HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
		attacks. Develop vulnerability management policies, evaluation standards, and management processes to implement full lifecycle management of security vulnerabilities. Vulnerability scanning programs are run periodically to detect potential security vulnerabilities in a timely manner and take countermeasures. l) Strictly select business partners and service providers, and incorporate personal data protection requirements into business contracts, audits, and appraisal activities. In addition, HUAWEI CLOUD has been certified by multiple international standards related to privacy compliance to ensure account data security, including ISO 27701, ISO 29151, ISO 27018, BS 10012, and SOC2TypeII privacy principle audit report. Customers can also learn about personal data security control in the HUAWEI CLOUD environment through HUAWEI CLOUD certification and reports.
Retention Limits PDPL: Article 8. Principle of quality PDPL Directive: Article 31. Provision of services or processing on request	Data shall not be retained for longer than the minimum time necessary for the purpose of processing. Personal data shall be retained for a maximum period of two (2) years from the date of the last order. Personal data may be retained for a period longer than the prescribed period only in the cases provided for in Article 30, paragraph 2, of the Act, or in the cases expressly provided for by the legislative provisions in force. In this case, the data must be returned to the controller for retention as long as the legal obligation persists. Unauthorized retention of personal data is generally prohibited.	1. HUAWEI CLOUD will retain customer account data within the period required for the purposes specified in the Privacy Policy Statement, unless the retention period needs to be extended according to legal requirements. 2. After a customer closes an account, HUAWEI CLOUD will stop providing services to the customer and delete the customer's account data within a reasonable period of time. The prerequisite is that the law does not require us to continue processing some customer account data, for example, for accounting or bookkeeping purposes, or to fulfill our

Basic obligations of regulations	Requirements for HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
		obligations. or exercise our rights under the agreement relating to the Services.
Transfer Restriction	When transferring data across borders, the data controller shall only transfer data to countries that provide an adequate level of data protection, except in the following cases: a) Data subjects' explicit authorization; b) the data controller transfers medical data for health or public health reasons; c) Transfers by a bank or stock exchange in accordance with applicable law; (d) Transmissions agreed on the principle of reciprocity within the framework of international treaties to which the Republic of Peru is a party; e) where authorised by the data controller, the transmissions necessary for the execution of a contract between the data subject and the data controller or the execution of pre-contractual measures; f) Transmissions that are legally necessary for the protection of the public interest or for the recognition, exercise or defence of a right in judicial proceedings.	Customer account data is stored on servers in Singapore by default. HUAWEI CLOUD provides services for customers through global resources. Therefore, the customer's account data may be transferred to the countries or regions where HUAWEI CLOUD affiliates and partners are located, or may be accessed by these countries or regions. In this case, HUAWEI CLOUD will ensure that such transfer complies with applicable legal requirements and passes strict internal review. For example, HUAWEI CLOUD will sign a data transfer agreement that provides sufficient protection for personal data, or inform customers of the necessity and potential risks of cross-border data transfer, and obtain customers' explicit consent.
Leakage Notice PDPL: Article 34. National Registry for the Protection of Personal Data Article 35. Confidentiality Article 36. Remedies of the National Authority for the Protection of Personal Data	Upon discovery of a personal data security incident, the National Data Protection Authority must be notified within 48 hours. If a security incident affects other rights of a data subject, the data subject must be notified within 48 hours, and detailed information about the incident and measures taken must be provided. Report to the supervisory authority any breach of security regulations that poses a risk to the management of the data subject's personal data.	HUAWEI CLOUD has set up a privacy protection team and developed the Requirements on Personal Data Breach Management to specify the personal data breach handling process, including pre-event prevention, incident identification, incident handling, and incident closure and recording. During incident handling, HUAWEI CLOUD generally notifies the supervisory authority of the personal data breach according to applicable laws and regulations after

Basic obligations of regulations	Requirements for HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
	Any security incidents must be documented in detail to ensure completeness and accuracy of the records.	identifying the breach. In addition, if HUAWEI CLOUD identifies that the personal data breach may cause high risks to the rights and freedoms of data subjects, property loss, and personal safety, HUAWEI CLOUD will notify the data subjects immediately.
Accountability obligations PDPL Directive: Article 37. Appointment of the Personal Data Office Article 40: Impact assessment relating to the protection of personal data Article 47. Security Document	Develop effective internal policies and procedures for personal data protection to comply with legal regulations and requirements.	1. HUAWEI CLOUD has developed and implemented policies on personal data protection and established a comprehensive privacy protection process system. Through a series of scientific and strict processes, HUAWEI CLOUD ensures that business activities comply with privacy protection requirements, such as privacy protection policies, privacy protection frameworks, and privacy protection design specifications. In addition, HUAWEI CLOUD regularly organizes training and publicize to improve employees' privacy protection awareness and skills. 2. HUAWEI CLOUD has appointed a Data Protection Officer (DPO) in accordance with applicable laws. In case of any questions, comments, suggestions, etc., the customer may contact the DPO via the contact details provided in the Privacy Policy Statement.

5.3 How HUAWEI CLOUD Complies with PDPL Requirements as a Data Processor

For customer data, HUAWEI CLOUD has released the Data Processing Addendum to clarify the data processing activities and obligations of HUAWEI CLOUD as a data (sub-) processor.

5.3.1 HUAWEI CLOUD Data Processing Activities

1. Roles of the Parties

1) If the customer is the data controller in the applicable privacy laws, HUAWEI CLOUD is the data processor in the applicable privacy laws.

2) If the customer is a processor of customer data in the applicable privacy laws, HUAWEI CLOUD is a sub-processor of customer data in the applicable privacy laws.

2. Processing Activities

a) **Object of processing：** The object of processing is customer data.

b) **Period of processing：** The period of processing is determined by the customer.

c) **Purpose of processing：** The purpose of the processing is to provide cloud services to the customer in accordance with the customer's instructions。

d) **Nature of processing：T**he nature of the processing is to provide the customer with functions such as computing, storage, transmission, processing, and deletion related to the cloud service.

e) **Types of Customer Data:** Types of Customer Data means information about individuals in Customer Content.

f) **Lawfulness of processing：** HUAWEI CLOUD processes customer data only according to customer instructions.

5.3.2 HUAWEI CLOUD fulfills Processor Obligations

1. Ensuring the security of customer data

HUAWEI CLOUD implements and maintains the following technical and organizational measures to ensure customer data security:

a) Set up a privacy protection organization to identify and manage personal data protection risks.

b) Develop data security and personal data protection policies, including security vulnerability response and data breach processes, are developed to reduce privacy security risks caused by personal data breaches and guide relevant departments to process personal data in compliance with laws and regulations.

c) Organize security and privacy protection training, testing, publicize, and other activities to improve employees' personal data protection awareness.

d) Implement a series of measures, such as entrance and exit control, access control system, and closed-circuit television (CCTV) system to ensure the physical security of the data center and prevent unauthorized access, damage, or interference to HUAWEI CLOUD infrastructure.

e) Deploy protection mechanisms such as anti-DDoS systems and intrusion detection systems to protect network from attacks. Develop vulnerability management policies, evaluation standards, and management processes to implement full lifecycle management of security vulnerabilities. Vulnerability scanning programs are run periodically to detect potential security vulnerabilities in a timely manner and take countermeasures.

f) Clearly define and assign cybersecurity roles and responsibilities, implement segregation of duties (SOD)based on risk assessments, mitigate risks, and protect data processing systems from unauthorized use.

g) Encrypt and pseudonymize personal data using recommended industry standard protocols, as appropriate, during data storage and transmission to prevent data breaches and unauthorized access.

h) Degauss the discarded storage media before returning them to the warehouse to ensure that the media are overwritten by software before being discarded to prevent data leakage. In cases where this is not possible (CDs, DVDs, etc.), physical destruction will take place.

i) implement appropriate operational security management and technical measures, including identity authentication and access control, change and event management, vulnerability management, configuration management, event logging, continuous monitoring of cybersecurity incidents and threats, timely detection of anomalies, and proactive measures to deal with them; ensure that personal data is not read, copied, altered or deleted by unauthorized persons.

j) In the authorization phase, identify data processing suppliers and sign a data protection agreement (DPA) with them to ensure that the suppliers, as sub-personal information trustees, can only process customer data according to the instructions of customers and take sufficient organizational and technical measures to protect customer data.

2. Obligations to notify and assist customers

HUAWEI CLOUD's obligations to notify and assist customers include:

a) Disclose the Customer Data Sub-Processor to the Customer and ensure that the Customer Data is processed by the Sub-Processor in accordance with the Customer's instructions.

b) HUAWEI CLOUD shall notify the customer of the data breach without undue delay. and assist the customer in ensuring compliance with the obligations required by applicable privacy laws based on the nature of the processing and the information provided by HUAWEI CLOUD.

c) HUAWEI CLOUD assists the Customer in fulfilling its obligations and responding to data subjects' requests for exercising their rights specified in applicable privacy laws. HUAWEI CLOUD will use commercially reasonable efforts to forward any request from a data subject who has received Customer Data to Customer in a timely manner.

d) Customer may elect to implement additional security controls to protect Customer Data based on Customer's business needs. Additional security control measures can be obtained from HUAWEI CLOUD or directly from third-party suppliers. HUAWEI CLOUD will provide the following convenience for customers to implement additional security control measures: (a) allow customers to take measures to protect customer data; and (b) provide Customer with information regarding the protection, access and use of Customer Data.

3. Obligations to assist in the cross-border compliance of customer data

HUAWEI CLOUD provides services and resources to help customers comply with applicable privacy laws and regulations on cross-border personal data transfer:

a) **HUAWEI CLOUD services locations：** HUAWEI CLOUD provides services in Peru, Chile, Brazil, Mexico, Singapore, China, Hong Kong, Thailand, South Africa, Indonesia, and Turkey. Customers can select cloud services in any of the preceding regions to store and process customer data.

b) **Location of customer data processing:** The location of customer data processing is the region where the Huawei cloud service selected by the customer is located. For example, if a customer selects the Peru region as its computing service resources, the customer data stored and processed by the customer in the computing service will reside only in the Peru region. HUAWEI CLOUD may transfer customer data out of the region selected by the

customer only in the following cases: (a) obtaining the customer's consent, or (b) complying with applicable laws and regulations as well as binding orders issued by courts or competent public authorities.

6 Customer Complies with the Requirements and Notices of Peruvian PDPL

6.1 Customer's Privacy Protection Responsibilities and Notices

When a customer selects and uses Huawei Cloud services to store and process customer data, the customer:

1) Determines the purpose of using customer data.
2) Determines how customer data is processed, for example, from whom and what customer data is collected.
3) Controls the access, update, and use of customer data.

According to applicable privacy laws, the customer is the customer data controller. The customer may need to comply with the following applicable privacy law requirements and precautions when fulfilling related legal obligations.

Basic obligations of regulations	Customer Specific Requirements	Notices
Basic obligations of regulations Notice and Consent PDPL Article 5. Principle of consent PDPL Directive： Article 1. Consent to the processing of personal data Article 2-6: Characteristics of valid consent	Follow the principles of legality, legitimacy, and necessity. When processing personal information based on personal consent, comply with relevant regulations, such as not collecting information beyond the scope or obtaining consent by misleading means. Before processing personal information, the individual shall be clearly informed of the processor's information, purpose, method, type, and retention period. Individual consent must be obtained for scenarios such as processing sensitive personal information and providing personal information to third parties. When the purpose,	1. The customer determines and understands from whom the customer data is collected, how it is collected, what type of customer data is collected, and how it is used, including the purpose of disclosing the customer data to third parties. Therefore, the customer shall: a） send a notice to the individuals to whom the Customer Data relates, informing them of the processing of the Customer Data

Basic obligations of regulations	Customer Specific Requirements	Notices
Article 13: Conditions for Transfer of Personal Data	method, or type of processing is changed, the consent must be obtained again.	as described above. b） If the Customer's legal basis for processing Customer Data is the consent of the individual, the Customer shall obtain the consent of the individual to whom the Customer Data relates. If the individual refuses to consent, the Customer shall cease collecting, using or disclosing his/her personal data. 2. If the customer selects and uses Huawei Cloud services to store and process customer data, the customer can notify the individuals related to the customer data. 3. HUAWEI CLOUD will only process customer data based on customer instructions. Customer data will not be collected or used for HUAWEI CLOUD purposes.
Purpose Limitation PDPL: Article 6. Principle of purpose Article 7. Principle of proportionality Article 13. Scope of the processing of personal data PDPL Directive: Article 26: Processing of data for advertising and commercial prospecting	Personal data must be collected for specific, clear, and legitimate purposes. The processing must respect the rights of data subjects and comply with the principle of proportionality. That is, the processing method must be appropriate for the purpose and not excessive. Data subjects' consent is required when personal data is processed for advertising and commercial promotion. No further contact or data processing shall be allowed without consent after the first contact.	1. The customer determines the collection, use purpose, and disclosure object of the customer data. The customer shall ensure that the collection method, use purpose, and disclosure object of the customer data are consistent with those notified to related individuals. 2. To provide customers with selected HUAWEI CLOUD services, HUAWEI CLOUD collects, uses, or discloses customer data only based on the functions provided by the services.
Data subject rights	During the processing of personal data, the rights of data subjects shall be fully and effectively guaranteed.	1. The customer determines who collects the customer data and who has the right

Basic obligations of regulations	Customer Specific Requirements	Notices
PDPL: Article 18-27 PDPL Directive: Article 63-87 Right of information\Right of access\ Right to update, inclusion, rectification and erasure\ Right to prevent the provision\ Right to object\ Right to objective processing	Right to know and access: Data subjects have the right to obtain all relevant information through access. Data portability: Where processing is based on consent or contract and is conducted by automated means, data subjects may request that their personal data be transmitted to other data controllers or responsible persons in a structured, common and machine-readable format. Right of correction, right of deletion or cancellation, right of objection: Data subjects have the right to request correction of inaccurate data; may request deletion or cancellation of data when the data is no longer necessary, when the processing period expires, when consent is withdrawn, etc.; The processing of their personal data can be opposed at any time, and the enterprise needs to stop the processing. Right to process data objectively: Data subjects have the right not to be involved in automated decisions that have significant impact.	to access or correct the customer data. Therefore, the customer should provide the data subject's rights or mechanisms, such as access and correction, for individuals related to the customer data. 2. To provide customers with selected HUAWEI CLOUD services, HUAWEI CLOUD will only support access to and correction of customer data based on the functions provided by the services. 3. HUAWEI CLOUD assists customers in fulfilling their obligations and responding to data subjects' requests for exercising their rights specified in applicable privacy laws. HUAWEI CLOUD will use commercially reasonable efforts to forward any request from a data subject who has received Customer Data to Customer in a timely manner.
Accuracy PDPL: Principle of quality	The personal data processed must be true, accurate and as up-to-date, necessary, relevant and sufficient as possible for the purposes for which the data were collected.	1. The customer owns and fully controls the customer data. The customer shall take necessary measures to ensure the accuracy of the customer data stored and processed by Huawei cloud services. 2. To provide customers with selected HUAWEI CLOUD services, HUAWEI CLOUD stores and processes customer data based only on the functions provided by the services. HUAWEI CLOUD will not modify or tamper with customer data.

Basic obligations of regulations	Customer Specific Requirements	Notices
Protecting PDPL: Article 9. Principle of security Article 16. Security of personal data processing Article 17. Confidentiality of personal data PDPL Directive: TITLE I PROCESSING OF PERSONAL DATA CHAPTER VI SECURITY MEASURE	Keep personal data under secure conditions to prevent it from being tampered with, lost, accessed, and used without authorization. Security assurance measures: Take necessary technical, organizational, and legal measures to ensure the security of personal data and prevent data from being tampered with, lost, processed, or accessed without authorization. Security measures shall be appropriate to the processing activity and the type of data. Data backup and recovery: Design and implement security control measures, including maintaining security areas, protecting devices, and ensuring that security backups are generated and verified. Backups are performed at least weekly unless the data is not updated and security measures are required for storage, transfer, and destruction. You need to verify the integrity of the backup data and restore the data in case of interruption or damage. Data transmission security: The exchange of personal data from the processing or storage environment to any destination outside the entity must be authorized by the data subject, using the means of transportation authorized by the data subject, and taking measures such as encryption, digital signature, and certificate to prevent unauthorized access, loss, or damage. Non-automated document storage: Facilities such as cabinets storing non-automated documents shall be protected by keys or other equivalent devices, data storage areas shall be closed when not necessary, keys or openers shall be formally assigned, and transfer and allocation procedures shall be in place. Document copying and destruction: Documents containing personal data must be generated or copied under the control of authorized personnel. Discarded copies must be destroyed	1. Customers are responsible for the security within the cloud services they use, including customer data. Therefore, customers should take measures to ensure the internal security of cloud services, such as hardening security configurations for cloud services, deploying security services such as virtual firewalls and API gateways, controlling customer data access permissions, and encrypting customer data for storage and transmission. 2. HUAWEI CLOUD is responsible for the security of the cloud platform and infrastructure. Therefore, HUAWEI CLOUD implements and maintains appropriate security measures to ensure the security of the cloud platform and infrastructure, including but not limited to: a） Implement a series of measures, such as entrance and exit control, access control system, and closed-circuit television (CCTV) system to ensure the physical security of data centers and prevent unauthorized access, damage, or interference to HUAWEI CLOUD infrastructure. b） Protection mechanisms such as anti-DDoS and intrusion detection systems are deployed to protect network from attacks. Vulnerability management policies,

Basic obligations of regulations	Customer Specific Requirements	Notices
	to prevent information access or subsequent recovery. Document access control: Document access is restricted to authorized personnel. A mechanism must be established to identify access to documents of multiple users. Access to documents by unauthorized personnel must be properly recorded. Non-automated document transfer: When transferring non-automated documents, take measures to prevent unauthorized access, misuse, manipulation, and modification of data.	evaluation standards, and management processes are formulated to implement full lifecycle management of security vulnerabilities. Vulnerability scanning programs are run periodically to detect potential security vulnerabilities in a timely manner and take countermeasures. c） Clearly define and assign cybersecurity roles and responsibilities and implement separation of duties (SOD) based on risk assessment to reduce risk and prevent unauthorized use of data processing systems. d） During data storage and transmission, personal data is encrypted or pseudonymized using recommended industry standard protocols, as appropriate, to prevent data leakage and unauthorized access. e） Discarded storage media is degaussed before being returned to the warehouse to ensure that the media is overwritten with software before disposal. Where this is not possible (CDs, DVDs, etc.), physical destruction should be carried out. f） Implement appropriate operational security management and technical measures, including identity authentication and access control, change and event management, vulnerability

Basic obligations of regulations	Customer Specific Requirements	Notices
		management, configuration management, event logging, etc., to continuously monitor cybersecurity incidents and threats, detect anomalies in a timely manner, and proactively take action; Ensure that personal data cannot be read, copied, tampered with, or deleted by unauthorized personnel.
Retention Limits PDPL: Article 8. Principle of quality PDPL Directive: Article 31. Provision of services or processing on request	Data shall not be retained for longer than the minimum time necessary for the purpose of processing. Personal data shall be retained for a maximum period of two (2) years from the date of the last order. Personal data may be retained for a period longer than the prescribed period only in the cases provided for in Article 30, paragraph 2, of the Act, or in the cases expressly provided for by the legislative provisions in force. In this case, the data must be returned to the controller for retention as long as the legal obligation persists. Unauthorized retention of personal data is generally prohibited.	1.The customer determines the purpose of using the customer data and has full control over the customer data. After the customer data has been used for the purpose and there is no legal requirement for retaining the customer data, the customer shall delete the customer data. 2.The customer determines the retention period of the customer data. Huawei cloud services provide the customer with the function configuration or API for deleting the customer content. The customer can delete the customer content by referring to the cloud service documentation.
Transfer Restriction	When transferring data across borders, the data controller shall only transfer data to countries that provide an adequate level of data protection, except in the following cases: a) Data subjects' explicit authorization; b) the data controller transfers medical data for health or public health reasons; c) Transfers by a bank or stock exchange in accordance with applicable law; (d) Transmissions agreed on the principle of reciprocity within the framework of international treaties to	1. HUAWEI CLOUD provides cloud services in Peru, Chile, Brazil, Mexico, Singapore, China, China Hong Kong, Thailand, South Africa, Indonesia, and Turkey. Customers can select cloud services in any of the preceding regions to store and process customer data. 2. Customer data is stored and processed in the region where the HUAWEI CLOUD service is located. For example, if a customer

Basic obligations of regulations	Customer Specific Requirements	Notices
	which the Republic of Peru is a party; e) where authorised by the data controller, the transmissions necessary for the execution of a contract between the data subject and the data controller or the execution of pre-contractual measures; f) Transmissions that are legally necessary for the protection of the public interest or for the recognition, exercise or defence of a right in judicial proceedings.	selects the Peru region as its computing service resources, the customer data stored and used by the customer in the computing service will reside only in the Peru region. HUAWEI CLOUD may transfer customer data out of the region selected by the customer only in the following cases: (a) obtaining the customer's consent, or (b) complying with applicable laws and regulations as well as binding orders issued by courts or competent public authorities. 3. According to applicable privacy protection laws, if the customer data storage and processing location selected by the customer involves cross-border transfer, the Cross-Border Transfer Agreement provided by HUAWEI CLOUD will automatically apply. Only the customer knows the export and import destinations of cross-border data transfer. Therefore, the customer needs to evaluate whether the Cross-Border Transfer Agreement meets cross-border compliance requirements and whether other supplementary measures need to be taken, for example, notifying the customer of the individuals related to the data and obtaining their consent.
Leakage Notice PDPL: Article 34. National Registry for the Protection of Personal Data	Upon discovery of a personal data security incident, the National Data Protection Authority must be notified within 48 hours. If a security incident affects other rights of a data subject, the data subject must be notified within 48 hours, and detailed	1. The customer determines from whom to collect personal data. Only the customer knows the individuals related to the customer data. If customer data is leaked, the

Basic obligations of regulations	Customer Specific Requirements	Notices
Article 35. Confidentiality Article 36. Remedies of the National Authority for the Protection of Personal Data	information about the incident and measures taken must be provided. Report to the supervisory authority any breach of security regulations that poses a risk to the management of the data subject's personal data. Any security incidents must be documented in detail to ensure completeness and accuracy of the records.	customer should take measures in a timely manner, such as assessing data breach risks and notifying regulators or individuals. Customers can establish relevant regulations or processes to effectively handle customer data breaches. 2. After learning that the customer data is leaked, HUAWEI CLOUD will notify the customer in a timely manner and provide necessary assistance for the customer to handle the customer data breach.
Accountability obligations PDPL Directive: Article 37. Appointment of the Personal Data Office Article 40: Impact assessment relating to the protection of personal data Article 47. Security Document	Develop effective internal policies and procedures for personal data protection to comply with legal regulations and requirements.	1. The customer determines the purposes of collecting, using, and disclosing customer data. The customer is responsible for establishing related privacy protection policies and processes, and ensuring that employees who process customer data understand and comply with the policies and processes. 2. HUAWEI CLOUD provides necessary assistance for the customer to fulfill accountability obligations. For example, HUAWEI CLOUD will use commercially reasonable efforts to forward any request from the data subject who receives the customer data to the customer in a timely manner. Provide customers with third-party certification or audit results of HUAWEI CLOUD.

6.2 How HUAWEI CLOUD Products and Services Help Customers Implement Content Data Privacy and Security

The customer is responsible for the security of customer data. To ensure the security of customer content, the customer can take additional security measures based on the security level of the customer content. The additional security measures can come from HUAWEI CLOUD or a third party.

HUAWEI CLOUD understands customers' privacy protection requirements and provides additional security measures for customers based on its rich privacy protection practices and technical capabilities. Additional security measures cover network, database, security, management, and deployment tools. The data protection, data deletion, network isolation, permission management, DR backup, and security audit functions of related products help customers enhance content security.

- Management and supervision

Product Name	Product Introduction	Core Functions
Identity and Access Management (IAM)	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.	Permission management
Cloud Trace Service (CTS)	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.	Security audit
Cloud Eye Service (CES)	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.	Security audit
Log Tank Service (LTS）	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	Security audit

Product Name	Product Introduction	Core Functions
	requirements. Customers can keep records of operations on personal data through LTS to guarantee the data owners' right to know.	

- **Security compliance**

Product Name	Product Introduction	Core Functions
Host Security Service (HSS)	Host Security Service (HSS) can provide asset management, vulnerability management, baseline checking, intrusion detection and other functions, which can help organizations more conveniently manage host security risks, detect and stop hacker intrusion behaviors in real time, as well as meet the requirements of compliance. Customers can use HSS to more conveniently manage the security risks of hosts and containers, and detect ransom, mining, penetration, escape and other intrusion behaviors in real time, as well as meet the requirements of compliance.	Asset management、 Vulnerability management、 Baseline check、 Intrusion detection
Web Application Firewall (WAF)	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. 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.	Security protection
Cloud Firewall (CFW)	Cloud Firewall (CFW) protects Internet and VPC borders on the cloud by real-time intrusion detection and prevention, global unified access control, full traffic analysis, log audit, and tracing. It employs AI for intelligent defense, and can be elastically scaled to meet changing business needs, helping you easily handle security threats. CFW is a basic service that provides network security protection for user services on the cloud.	Asset Protection、 Access Control、 Online Defense
Database Security Service (DBSS)	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. Customers can use DBSS to detect potential risks and ensure the security of their databases.	Security audit

Data Encryption Workshop (DEW)	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. Customers can use DEW for centralized key lifecycle management to ensure the integrity of data storage procedures.	Data encryption
Anti-DDoS Service (AAD)	Advanced Anti-DDoS (AAD) is a value-added security defense service that defends against large volumetric DDoS attacks on Internet servers. Customers can configure AAD to divert the attack traffic to high-defense IP addresses with significant defense capabilities for scrubbing, keeping customers' business stable and reliable.	Security protection
Data Security Center (DSC)	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. 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.	Data classification、 Data anonymization、 Data watermarking
Cloud Bastion Host (CBH)	CBH is a 4A (AAAA) unified security control platform from HUAWEI CLOUD that provides organizations with O&M management services integrating single sign-on (SSO), unified asset management, multi-terminal access protocols, file transfer, session collaboration, and other functions. Customers can remotely operate and maintain cloud hosts through CBH to improve customers' access control security capabilities, protect the security of resource operation and system management, and reduce the risk of illegal invasion of systems and O&M resources.	Permission management
Cloud Certificate Manager (CCM)	Cloud certificate Manager (CCM) is a cloud service that provides one-stop lifecycle management of digital certificates including SSL certificate and private certificate. Customers can use CCM to improve the confidentiality and security of SSL certificates and private certificates, improve the security of	Certificate management

	access and transmission channels, and reduce the risk of unauthorized data intrusion, access, or theft during transmission and access.	
SecMaster	Security Cloud Brain, based on cloud - native security, offers comprehensive capabilities for log collection, security governance, intelligent analysis, situational awareness, and orchestrated response. These capabilities form a rapid closed - loop Security Information and Event Management system. It achieves automated security operations, helping customers protect their cloud security.	Situation Awareness Security Operations

- **Network**

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

- **Storage**

Product Name	Product Introduction	Core Functions
Cloud Backup and Recovery (CBR)	Cloud Backup and Recovery (CBR) provides a unified backup services for Huawei Cloud servers, disks, databases, desktops, SFS Turbo file systems, as well as files and directories on local and cloud servers to protect against viruses, accidental deletions, and software or hardware faults.	Data backup
Volume Backup Service (VBS)	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. VBS can reduce the possibility of virus attack, human error deletion as well as hardware or software failure, protect data security and	Data backup

Product Name	Product Introduction	Core Functions
	reliability, and reduce the risk of data tampering.	
Cloud Server Backup Service (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 backup

7 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.

For more information on HUAWEI CLOUD security compliance and downloading relevant compliance Certification please refer to the official website of HUAWEI CLOUD "Trust Center - Compliance"

Certification	Description
ISO27001	ISO 27001 is a widely used international standard that specifies requirements for information security management systems. This standard provides a method of periodic risk evaluation for assessing systems that manage company and customer information.
ISO27017	ISO 27017 is an international certification for cloud computing information security. The adoption of ISO 27017 indicates that HUAWEI CLOUD has achieved internationally recognized best practices in information security management.

Certification	Description
ISO27018	ISO 27018 is the first international code of conduct that focuses on personal data protection in the cloud. This certification indicates that HUAWEI CLOUD has a complete personal data protection management system and is in the global leading position in data security management.
TL 9000& ISO 9001	ISO 9001 defines a set of core standards for quality management systems (QMS). It can be used to certify that an organization has the ability to provide products that meet customer needs as well as applicable regulatory requirements. TL 9000 is a quality management system built on ISO 9001 and designed specifically for the communications industry by the QuEST Forum (a global association of ICT service providers and suppliers). It defines quality management system specifications for ICT products and service providers and includes all the requirements of ISO 9001. Any future changes to ISO9001 will also cause changes to TL 9000. Huawei Cloud has earned ISO 9001/TL 9000 certification, which certifies its ability to provide you with faster, better, and more cost-effective cloud services.
ISO 20000-1	ISO 20000 is an international recognized information technology Service Management System (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure cloud service providers (CSPs) can provide effective IT services to meet the requirements of customers and businesses.
ISO22301	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
CSA STAR Certification	The Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider, developed CSA STAR certification. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
ISO27701	ISO 27701 specifics requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.
BS 10012	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
ISO29151	ISO 29151 is an 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.

Certification	Description
PCI DSS	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.
PCI 3DS	The PCI 3DS standard is designed to protect 3DS environments that perform specific 3DS functions or store 3DS data and support 3DS implementation. Passing the PCI 3DS certification shows that HUAWEI CLOUD complies with security standards in the process, flow, and personnel management of the 3D protocol execution environment.
ISO 27799	ISO/IEC 27799 provides guidelines on how organizations in the healthcare industry can better protect the confidentiality, integrity, traceability, and availability of personal health information. Huawei Cloud is the world's first cloud service provider to earn ISO/IEC 27799 certification. This certifies Huawei Cloud's deep understanding of intelligent applications for the healthcare industry, and its ability to protect the security of personal health information.
ISO 27034	ISO/IEC 27034 is the first ISO standard for secure programs and frameworks. It clearly defines risks in application systems and provides guidance to assist organizations in integrating security into their processes. ISO/IEC 27034 provides a way for organizations to verify their own product security and make security a competitive edge. This standard also outlines a compliance framework at the application layer for global cloud service providers, promoting the security of the R&D process, applications, and the cloud. Huawei Cloud is the world's first cloud service provider to obtain ISO/IEC 27034 certification. This marks a big step forward for Huawei Cloud governance and compliance.
SOC Audit Report	The SOC audit report is an independent audit report issued by a third-party auditor 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.

8 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.

In order to ensure that the business conducted in each region complies with the requirements of local privacy protection 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 privacy 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 Peru privacy regulations when using HUAWEI CLOUD.

9 Version History

Date	Version	**Description**
2025-5	2.0	Compliance requirement update
2024-8	1.1	Routine Update
2021-11	1.0	First Release