HUAWEI CLOUD Compliance with Argentina PDPL

Issue 1.0

Date 2020-12-16

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

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 Argentina.

1.2 Purpose of Publication

This document is intended to help customers understand:

1. HUAWEI CLOUD's privacy protection responsibility model;
2. Argentina Personal Data Protection Act 25,326 (PDPL) and related legal requirements;
3. The compliance of HUAWEI CLOUD with PDPL, as specified in the responsibility model;
4. HUAWEI CLOUD's controls and achievements in privacy management;
5. Customers' responsibilities and obligations when falling under the jurisdiction of PDPL, as specified in the responsibility model;
6. How to leverage HUAWEI CLOUD's security products and services to achieve privacy compliance.

1.3 Basic Definitions

- **HUAWEI CLOUD**

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

- **Customer**

  Registered users having a business relationship with HUAWEI CLOUD.

- **Personal Data**

  Information of any kind referred to certain or ascertainable physical persons or legal entities.

- **Sensitive Data**

  Personal data reveals the data owner's racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information on health, sexual habits or behaviors.

- **Data Processing**

  Systematic operations and procedures, electronic or not, that allow the collection, retention, management, storage, modification, relationship, evaluation, blocking, destruction, and in general the processing of personal data, as well as their transfer to third parties through communications, queries, interconnections or transfers.

- **Data Owner**

  Any physical person or legal entity having a legal address or delegations or branches in the country, whose data are subject to the treatment referred to in this Act.

- **Data User**

  Any person, either public or private, performing in its, his or her discretion the treatment of data contained in files, registers or banks (hereinafter referred to as platforms, systems, or other cloud services provided by HUAWEI CLOUD), owned by such persons or to which they may have access through a connection.

- **Data Dissociation**

  Treatment of personal data in such a way that the information obtained cannot be associated with any certain or ascertainable or determinable person.

- **Account Information**

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

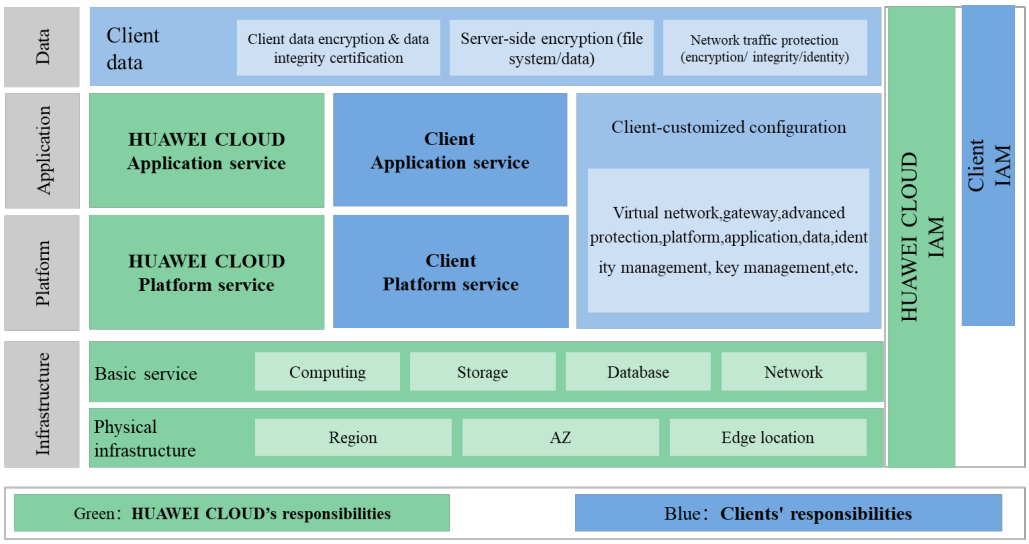
- **Content Data**

  Content stored or processed during the use of HUAWEI CLOUD services, including but not limited to data, documents, software, images, audio and video files. Content data may contain personal data, and as for the personal data in the content data, the customer act as the data user.

2 Cloud Services Privacy Protection Responsibilities Sharing Model

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

Figure 2-1 Responsibility Sharing Model



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

HUAWEI CLOUD: As the Cloud Service Provider (CSP), HUAWEI CLOUD is not only responsible for the security of personal data collected or processed during business operations and compliance, but also responsible for the **platform security**, which means providing secure and compliant infrastructure, cloud platform and software applications related to cloud services to customers.

- **Protection of Customer's Privacy**: HUAWEI CLOUD identifies and protects customers' personal data. HUAWEI CLOUD formulates privacy protection policies from company policies, processes and operation levels and adopts active privacy control measures, such as anonymization, data encryption, system and platform security protection, and comprehensively protect the security of customers.
- **Platform and Customer Security Support**: HUAWEI CLOUD is responsible for the security and compliance of the platform and infrastructure involved in the cloud service, ensuring the applications' security and platform security levels to comply with the requirements of applicable privacy protection laws and regulations. At the same time, HUAWEI CLOUD provides customers with a variety of privacy protection technologies and services, such as access control, identity authentication, data encryption, logging and auditing functions, in order to help customers protect their privacy according to their commercial requirements.

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

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

3 Overview of Argentina Privacy Laws

3.1 Background of Argentina Privacy Laws

PDPL, which is approved by the Argentine Parliament on October 30, 2000, applies to the processing of personal data in Argentina for individuals or legal entities (the latter needs to be located in Argentina or have offices or branches in Argentina). Its purpose is providing comprehensive protection to personal data in data files, registers, databases, or data banks or other technical data processing measures.

PDPL has been effort for a long time and the concept of cloud computing was first introduced 6 years after the legislation was passed which is in 2006. As to the similarity between cloud service models and data files, registers, databases or data banks mentioned in PDPL, HUAWEI CLOUD properly protects personal data that collected and contained in customer's content data according to PDPL requirements.

In addition to PDPL, Argentine Regulators have issued a number of specific resolutions and guidelines to help data users better meet the requirements of PDPL. A more central document is Resolution 47/2018 promulgated by the Argentine Acquisition of Public Information Agency (AAPI) on July 23, 2018. Resolution 47/2018 aims to promote data user's further compliance with PDPL-related requirements and to provide recommendations for security measures for the management, planning, control and continuous improvement of information security.

3.2 Core Regulatory Requirements of PDPL

PDPL specified the following core regulatory requirements for processing personal data.

- **Ensure the Quality of Personal Data**

  To ensure the quality of personal data, Article 4 of PDPL makes relevant provisions, mainly including the appropriateness of purposes, legal and legitimate, purpose limitation, data accuracy, data correction, data access and data retention restriction.

- **Notify and Obtain Consent**

  Whenever the data user requires the data owner to provide personal data, the data user should inform the data owner in advance that the purpose of data processing, the identity and type of the data user, the consequences of not providing or providing inaccurate data, and the rights of the data owner to access, correct, and delete the data. Notifications sent to the data owner must be in writing or in a similar manner, and the data user cannot process the personal data until they have the explicit consent from the data owner.

- **Collect and Process Sensitive and Medical Data Conditionally**

  The data user cannot force the data owner to provide sensitive data. Sensitive data can only be collected and processed for statistical and scientific purposes which are authorized by law when public interests are taken into considerations or data owners cannot be identified. It is prohibited to store the information that may disclose sensitive data directly or indirectly under PDPL. Medical data can be collected from patients only when medical institutions and medical research institutions provide patient medical services.

- **Ensure Data Security**

  The data user must take necessary technical and organizational measures to protect personal data from changes, losses, unauthorized access or processing, and fully protect the security and confidentiality of personal data.

- **Confidentiality Obligations**

  Data users and all persons participating in any stage of personal data processing are responsible for the confidentiality of personal data. Even if they no longer act as data users or participate in personal data processing, they still hold responsible of confidentiality.

- **Consent Related to Data Transfer**

  Processed Personal data can only be transmitted when it is directly related to the legitimate interests of data users and personal data receivers, given that the data owner is informed of the purpose of such data transfer and consented to. The recipient has the same obligations as the data user.

  The data owner's consent of data transfer is revocable. When data transfers occur directly between governments or data dissociation measures have been taken, data users do not need to obtain data owner's consent.

- **Conditional Cross-Border Transfer**

  With the exception of international judicial cooperations, epidemiological investigation needs, international cooperation to combat crime, and Argentina's special international treaty on relevant transfer, PDPL prohibits the transfer of any type of personal data to countries, international organizations, or supranational entities that cannot provide an adequate level of protection.

- **Requirements for Information Registration**

  PDPL requires data users or person who are responsible for personal data files, databases or registers to register relevant information with registries established by local regulatory bodies. The registered information includes the name and address of the person in charge, the purpose of collecting personal data, the nature of collecting personal data, the methods of collecting and updating personal data, the means of ensuring data security and possible transfer of destination of personal data, etc.

- **Time Limitation of Data Retention**

  Data users shall delete stored personal data in time after fulfilling their contract obligations. Personal data could be retained no longer than two years under reasonable assumptions about possible future services.

- **Data Processing Restrictions for Directing Marketing**

  Data users can only send e-marketing business information to data owners under specific circumstances, such as when personal data can be obtained in public documents, data owners provide it on their own initiative, and data users have obtained data owners' consent.

3.3 Security Measures Requirements of Resolution 47/2018

AAPI, the Argentine data protection authority, issued Resolution 47/2018 in 2018, which stipulates that data users should take necessary technical and organizational measures to ensure the security and confidentiality of their personal data. The resolution starts from eight control areas: data collection, access control, change control, backup and recovery, vulnerability management, data deletion, security incidents and development environment, setting out 30 specific security protection objectives in accordance with international standards and corresponding recommended security control measures.

3.4 Roles under PDPL

Two roles are defined by PDPL, which are the data owner and the data user.

The data owner is the owner of personal data and has the rights to know, access, recall, correct and update the data and restrict data processing granted by PDPL.

The data user is responsible for the collected personal data, ensure that collecting, processing, protecting and transmitting data owners' personal data based on the core requirements of the PDPL (refer to Chapter 3.2), and shall also comply with official documents such as Resolution 47/2018 and other resolutions, good practice guidelines issued by regulatory bodies.

3.5 The Role of HUAWEI CLOUD under PDPL

Personal data processed by HUAWEI CLOUD mainly includes personal data in customer's content data and personal data provided by customers when creating or managing HUAWEI CLOUD accounts.

When processing personal data in the customer's content data, the customer, as a data user, assumes the obligations set for the data user by PDPL. HUAWEI CLOUD will only process content data in accordance with customer's instructions, keep the data confidential and take appropriate security measures to protect customer content data security.

When a customer performs operations on HUAWEI CLOUD platform, including but not limited to registering, services purchasing, real-name authentication and service support, HUAWEI CLOUD will collect some personal data, such as the

customer's name, address, ID number, bank accounts information, and other types of information according to the service used. HUAWEI CLOUD, acting as the data user, is responsible for the security and privacy protection of customers' personal data, ensuring that the collection, processing and storage procedures comply with legal requirements, and adequately responding to data owners' requests.

4 How HUAWEI CLOUD Responses to the Requirements of Argentina PDPL and Implementing Regulations

4.1 HUAWEI CLOUD Privacy Commitment

HUAWEI CLOUD has placed cyber security and privacy protection as top priorities. HUAWEI CLOUD has integrated cyber security and privacy protection into its cloud services promising to provide customers with stable, reliable, secure, trustworthy, and evolvable services while respecting and protecting customers' privacy.

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

4.2 HUAWEI CLOUD Basic Privacy Protection Principles

- **Lawfulness, Fairness and Transparency**

  HUAWEI CLOUD processes personal data of data owners lawfully, fairly and in a transparent manner.

- **Purpose Restriction**

  HUAWEI CLOUD collects personal data for specific, explicit and lawful purposes and will not further process the data in a manner that is incompatible with those purposes.

- **Data Minimization**

  When HUAWEI CLOUD processes personal data, personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed. Personal data will be anonymized or pseudonymized to the extent possible to reduce the risks for data owners.

- **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.

- **Minimize Storage Duration**

  Personal data shall not be retained beyond the period necessary for the purposes of data processing.

- **Integrity and Confidentiality**

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

- **Accountability**

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

4.3 HUAWEI CLOUD's Compliance Measures in Response to PDPL

Based on the characteristics of HUAWEI CLOUD's business and the requirements of PDPL, HUAWEI CLOUD, as a data user, actively responds to and fulfills its obligations **when managing customer account information**. It adopts the following privacy protection mechanisms and technologies to comply with the core requirements of personal data utilization stipulated by PDPL.

Core Requirements of PDPL	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
Ensure the Quality of Personal Data	**Purpose Appropriateness:** Personal data collected and processed must be for defined, appropriate, and related processing purposes. **Legal and legitimate :** Data collection shall not be conducted by means that is unfaithful, fraudulent or in violation of PDPL regulations. **Purpose Restriction:** Personal data collected and processed must not be used for purposes inconsistent with or beyond the scope of collection. **Data Accuracy:** Data should be accurate, and updated when necessary. **Data Correction:** For all inaccurate or incomplete data, the user of personal data should disables/ deletes or replaces it after receiving the information. **Data Access:** Data consumers should ensure that data owners have access to personal data that they are collecting or processing. **Data Retention Restrictions:** Destroy data once it is no longer needed or irrelevant to the purpose of collection	At its core, HUAWEI CLOUD collects and processes personal data based on the purposes disclosed in the ***"Privacy Policy Statement"***. HUAWEI CLOUD regularly conducts Privacy Impact Assessments for products and services that involve personal data in order to prevent the collection and processing of personal data in products and services from exceeding the scope required for their actual purposes. HUAWEI CLOUD provides customers with a convenient channel to exercise data owner's rights. Customers can initiate requests to access or modify their incorrect or incomplete personal data through their mailboxes, as indicated in the ***"Privacy Policy Statement"***. HUAWEI CLOUD will provide customers with copies of the personal data they query or update, replace or discard incomplete or inaccurate information as requested after verifying the identity of the requester. HUAWEI CLOUD regularly audits the purposes of collecting, using and disclosing personal data, and performs security processing such as data dissociation or deletion of the personal data that is no longer needed. Customers can use the Close Account function in the Official Gateway to delete data stored in the HUAWEI CLOUD.

Core Requirements of PDPL	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
Notifying and Obtaining Consent	**Notifications:** When collecting personal data, the data owner should be notified in a clear and explict way in advance, including the purpose of data processing, the identity of the person who receives the data, the consequences of inaccurate or failure in data provision, and the rights of the data owner. **Explicit consent:** The notice must be presented to the data owner in writing or other equivalent manner, either explicitly or prominently, before data can be collected and processed with the consent of the data owner.	The ***"Privacy Policy Statement"*** introduces how HUAWEI CLOUD will collect and process customer's personal data, inform them whether they must provide data, the consequences if the data owner fails to provide the data, the purpose of data use, types of the objets regarding the data transfer , and the rights of data owners. When a customer registers for an account, HUAWEI CLOUD will clearly show the ***"Privacy Policy Statement"*** to the customer on the official website. The customer needs to click on the Confirm button to agree to the ***"Privacy Policy Statement"***. Additional privacy notices will be provided in the product agreement and get the customer's consent again if the purchased or after-sales service of the related product involves the collection or use of personal data for purposes other than those originally stated in the privacy statement. When the scope or use purpose of personal data collected by a product or service changes, the privacy statement will be updated accordingly and customers will be asked again for their consent.

Core Requirements of PDPL	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
Ensure Data Security	Data users must implement reasonable and appropriate organizational and technical measures to protect personal data from changes, loss, and unauthorized access and processing. Data users should store personal data in an environment that complies with technical integrity and security.	HUAWEI CLOUD uses a variety of management and technical controls to protect the security of personal data. **Organizational Security Measures:** HUAWEI has set up a global cyber security and privacy protection officer who is responsible for the formulation and implementation of HUAWEI's privacy protection policy . HUAWEI CLOUD has set up a team of privacy protection experts, including privacy protection experts, legal personnel, and network and information security professionals, to provide professional support for HUAWEI CLOUD privacy protection strategy and practice. For countries and regions where it operates, HUAWEI CLOUD assigns dedicated legal and privacy protection personnel to help HUAWEI CLOUD implement local activities in compliance with applicable privacy laws and regulations. HUAWEI CLOUD has established a privacy protection governance framework covering all businesses, and through a series of privacy protection processes, to support business activities to meet privacy protection requirements, such as data owners' rights protection, emergency response to data breaches, and personal data retention, etc. HUAWEI CLOUD retains complete records of any personal information processing activities performed

Core Requirements of PDPL	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
		by HUAWEI CLOUD. Every service lists the type of data owners, the type of personal data, the collection purpose, the transfer of personal data, retention period and security measures etc. through conducting privacy impact assessments. **Physical security measures:** HUAWEI CLOUD has established comprehensive physical security and environmental safety protection measures and strategies. In addition, the HUAWEI CLOUD O&M team enforces stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to protect the physical security and environmental safety HUAWEI CLOUD data centers. **Technical security measures:** Authentication: strict password policy and multi-factor authentication are adopted; Permission management: role-based access control and permission management for operation and maintenance personnel is implemented; Data storage and transfer: sensitive data encryption is adopted; Risk monitoring: logging and auditing of data processing is adopted to monitor and audit the access to the key systems. **Security certification:** In addition, customers can also understand the privacy security controls within HUAWEI CLOUD's environment through

Core Requirements of PDPL	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
		HUAWEI CLOUD security reports or certifications. HUAWEI CLOUD has obtained multiple certifications in relation to privacy compliance international standard, including ISO 27701, ISO 29151, ISO 27018, BS 10012, SOC2 Type1, privacy audit reports., etc. (Detailed certification is described in Chapter 6). ISO 27018 is the International Code of Conduct focused on personal data protection in the cloud. The pass of ISO 27018 indicates that HUAWEI CLOUD has a complete personal data protection management system.
Confidentiality Obligations	All persons participating in personal data processing or data users shall maintain strict confidentiality of personal data that they have come into contact with.This obligation should continue to be fulfilled even if they no longer participate in the processing of personal data.	HUAWEI CLOUD makes that all employees' qualifications, capabilities, and behavior comply with privacy protection requirements from various aspects and requires employees to pass privacy protection related assessment every year. In addition, HUAWEI CLOUD has identified privacy protection related positions and clearly defined the responsibilities of these positions. HUAWEI CLOUD also conducts background investigation and skill assessment for new employeesto help that they meet the requirements. All employees shall participate in the training on privacy protection awareness and pass the assessment . When an employee is repositioned, related permissions will be canceled.

Core Requirements of PDPL	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
Consent Related to Data Transfer	Personal data processed can only be transmitted if the legitimate interests of the data user and the personal data recipient are directly related, and the data owner is informed of the purpose and consent of such data transfer.	In the ***"Privacy Policy Statement"***, HUAWEI CLOUD explains the use of personal data (purpose, third party information, etc.) and obtains the consent from data owners. To provide customers with the necessary transaction, service and security support, HUAWEI CLOUD may share some personal data with third parties, i.e., affliated companies, branches, service providers, subcontractors, cooperation partners, etc. When transferring personal data to a third party, HUAWEI CLOUD uses encrypted channels in order to protect the personal data security.
Consent to Cross-Border Transfer	Except in exceptional cases, cross-border transfer of personal data should only be carried out when it is confirmed that the transmitting country or international organization has sufficient level of protection for personal data.	HUAWEI CLOUD has set up a team of privacy experts to estimate the level of personal data protection provided by the countries involved in data transfer. For the countries and regions where it operates, HUAWEI CLOUD also has full-time legal and privacy protection personnel to help HUAWEI CLOUD take necessary measures in accordance with applicable privacy laws and regulations.

Core Requirements of PDPL	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
Information Registration Requirements	Before processing the content data, relevant information should be registered with the registry established by the local regulatory authority, including the name and address of the person in charge, the purpose of collecting personal data, the characteristics of personal data collection, the methods of collecting and updating personal data, the means of ensuring data security, and the destination of possible transfer of personal data.	According to the requirements of ISO27001 standard, HUAWEI CLOUD has assigned special personnel to keep in touch with industry organizations, risk and compliance organizations, local authorities and regulatory agencies and establish contact points. HUAWEI CLOUD has set up special posts to maintain positive contact with external parties to pay attention to the dynamics of laws and regulations.
Time Limitation of Data Retention	After fulfilling the contractual obligations, the stored personal data shall be deleted in a timely manner. Personal data can be retained for up to 2 years when it is reasonably inferred that services may be provided in the future.	When customers actively delete data or need to delete data due to service expiration, HUAWEI CLOUD will strictly follow the data destruction standard and the agreement with customers to delete the stored customer data.

Core Requirements of PDPL	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
Data Processing Restrictions for Direct Marketing	E-marketing business information should only be sent to data owners under specific circumstances, such as personal data can be obtained in public documents, provided by data owners on their own initiative, and the consent of data users has been obtained.	Customers can choose whether to agree to use personal data for marketing when registering the account number of HUAWEI CLOUD official website. Only after obtaining the consent of the customer, as the data owner, can HUAWEI CLOUD send the promotion information to the customer. Only after the customer agrees to the direct marketing, HUAWEI CLOUD can sends the promotion information to the customer by SMS or email. If the customer decides to terminate the consent on using his/her personal data for direct marketing, it can be modified in the message reception configuration of the user center.

4.4 HUAWEI CLOUD's Compliance Measures in Response to Resolution 47/2018

HUAWEI CLOUD actively takes various types and dimensions of control measures to ensure the security of data. According to the requirements of Resolution 47/2018, HUAWEI CLOUD fulfills the obligations of personal data users to protect personal data security during collecting, accessing, changing, developing, destructing and security incidents occurring. The specific measures are as follows:

- Data Collection

Purposes	Brief Introduction of Controls	Measures Taken by HUAWEI CLOUD
A.1 Integrity	A.1.1 To Ensure Data Completeness	HUAWEI CLOUD has developed a data security specification, which standardizes the hierarchical management and control requirements of data collection and transfer, and uses reasonable encryption technology to detect the integrity of important data transfer process. HUAWEI CLOUD according to the data classification standard, use the corresponding encryption technology for different levels of data to protect the integrity of the data.
	A.1.2 Minimize Input Errors	HUAWEI CLOUD has designed different data input strategies for the types of data collected, which limits the format, number of bits and character requirements of user input data, and reduces the possibility of input errors.
	A.1.3 To Ensure Data Accuracy	HUAWEI CLOUD has a data verification mechanism, which checks the input data such as mobile phone number and email address through the verification code to verify that the collected data is accurate and effective.
A.2 Confidentiality	A.2.1 To Warrant Confidentiality During the Entire Data Collection Process	HUAWEI CLOUD has established a scientific and effective management system that can systematically and continuously manage security risks and ensure data confidentiality, integrity, and availability of itself and customers, , and HUAWEI CLOUD has passed the ***CSA STAR Gold Certification***.
	A.2.2 To Restrict Access to Data Collection	HUAWEI CLOUD has established strict password policy and enables multi-factor authentication to strictly control the access to the collection process. At the same time, HUAWEI CLOUD uses IAM access control and identity authentication technology to manage the access control of the access collection process, and uses encryption technology for the transfer channel to restrict unauthorized access to the collection process.
	A.2.3 To Restrict Unauthorized Access During Collection	

- Access Control

Purposes	Brief Introduction of Controls	Measures Taken by HUAWEI CLOUD
B.1 Identification of Assets	B.1.1 Identify Assets	HUAWEI CLOUD's information asset classification is monitored and managed by special tools to form an asset list, and each asset is assigned an owner. For personal data, HUAWEI CLOUD use Privacy Impact Assessment (PIA) regularly combing the list of personal data assets and identifies the corresponding asset owner. HUAWEI CLOUD checks the control effect through internal and external audit. Internal audit continuously tracks the effectiveness of security control measures, while external audit who act as an independent auditor review the efficiency and effectiveness of implemented security controls.
	B.1.2 Identify Responsible Parties and Determine Their Responsibilities	
	B.1.3 Verify the Controls Application	HUAWEI CLOUD has an access control mechanism, which provides each employee with a unique identity and divides permissions according to employee's job responsibilities. It also records the access to key systems through log records and audit technology, and manages privileged accounts through regular monitoring and auditing.

Purposes	Brief Introduction of Controls	Measures Taken by HUAWEI CLOUD
B.2 Access of Data	B.2.1 Manage Access to Systems	HUAWEI CLOUD has established access control management requirements according to ISO27001, followed the principle of minimum authority and separation of authority, regularly reviewed the scope of employees' rights, and avoided the permission beyond its scope of work. The employee shall verify their identity at each login to HUAWEI CLOUD, and the log can be traced back to the staff for accountability in case of an accident. When an employees' on-the-job status changes, the permissions shall be cleaned and modified in time. Logs of employees' logins and operations will be kept for the required time to respond to the audit requirements.
	B.2.2 Assign Permission	HUAWEI CLOUD has established comprehensive physical security and environmental safety protection measures, strategies, and procedures . HUAWEI CLOUD enforces stringent data center access control for both personnel and equipment. Security guards, stationed 24/7 at every entrance to each HUAWEI CLOUD data center site as well as at the entrance of each building on site, are responsible for registering and monitoring visitors and staff, managing their access scope on an as-needed basis. Different security strategies are applied to the physical access control systems at different zones of the data center site for optimal physical security. HUAWEI CLOUD data centers employ industry standard data center physical security technologies to monitor and eliminate physical hazards and physical security concerns. CCTV monitoring is enabled 24/7 for data centers' physical perimeters, entrances, exits, hallways, elevators, and computer cage areas. CCTV is also integrated with infrared sensors and physical access control systems. Security guards routinely patrol

Purposes	Brief Introduction of Controls	Measures Taken by HUAWEI CLOUD
	B.2.3 Verify the Identification and the Authorization	data centers and set up online electronic patrol systems such that unauthorized access and other physical security incidents promptly trigger sound and light alarms.HUAWEI CLOUD assigns permissions to employees according to the minimum scope of working needs. The access and modification of the information security management system and sensitive information are under monitored and recorded. Access to all ports, applications, system components, etc. are only open to authorized individuals and applications.
	B.2.4 Control Physical Access to Data Centers	Strictly following the international and national standards, HUAWEI CLOUD carries out site selection, design, and construction of data centers (DCs), and implements hierarchical security protection for data centers, from the fence to the DC building, and from the DC building to modules, from modules to cabinets, from cabinets to servers, to ensure the physical and environmental security of cloud DCs. In the meantime, 24x7 monitoring is enabled to detect and eliminate potential risks to ensure stable running of DCs.
	B.2.5 Monitoring Activities	HUAWEI CLOUD has access rights management mechanism, which strictly controls the access to personal data, and immediately removes the permission when it is not needed. At the same time, HUAWEI CLOUD monitors access to sensitive data through logging and auditing technology.
	B.2.5 Monitoring Activities (Sensitive data)	

- Change Control

Purposes	Brief Introduction of Controls	Measures Taken by HUAWEI CLOUD
C.1 Change Control	C.1.1 Ensure Changes	HUAWEI CLOUD has a configuration and change management mechanism. It adopts a unified change management

Purposes	Brief Introduction of Controls	Measures Taken by HUAWEI CLOUD
	C.1.1 Ensure Changes (Sensitive Data)	process for the changes of various elements of the production environment, such as computer room facilities, network, system platform software and hardware, and application. The change can only be carried out after application, environmental test and other verification tests and security reviews, so as to improve the integrity, availability and confidentiality of data.

- Backup and Recovery

Purposes	Brief Introduction of Controls	Measures Taken by HUAWEI CLOUD
D.1 Backup Copies and Recovery Procedure	D.1.1 Ensure a Formal Backup and Recovery Procedure	HUAWEI CLOUD has a backup strategy. It will regularly back up personal data, and regularly test the effectiveness of the backup of personal data in the system, and keep the records of the backup test.
	D.1.2 Ensure Access Control	HUAWEI CLOUD has access control mechanism, which controls the access rights and physical access to the server or computer room storing personal data backup and the environment for backup recovery test, and encrypts the stored backup by integrating with data encryption service.
	D.1.2 Ensure Access Control (Sensitive Data)	

- Vulnerability Management

Purposes	Brief Introduction of Controls	Measures Taken by HUAWEI CLOUD
E.1 Vulnerability Management	E.1.1 Prevent Security Incidents by Design	HUAWEI CLOUD has built a unified analysis and early warning platform to comprehensively grasp the data security situation, quickly identify and respond to security incidents. At the same time, through the correlation analysis of alarm, incident, asset and other information, risk assessment and security situation prediction can be carried out, so as to formulate security protection strategies in advance, so as to prevent in the bud.
	E.1.2 Ensure Proper Protection	HUAWEI CLOUD deploys Anti-DDoS devices on the Internet boundary to detect and clean abnormal and ultra-large traffic attacks. Intrusion prevention devices are deployed at the border of key network zones to identify attacks from the Internet and customers and automatically block these attacks. All cloud platform hosts of HUAWEI CLOUD are installed with security protection software for weak password detection, configuration management, intrusion detection and emergency response to build a compliant and secure host environment. HUAWEI CLOUD implements physical separation and encryption for production, test and development environment, and has a complete access control mechanism to manage access to different environments. HUAWEI CLOUD has a complete security event management mechanism and established an event management platform. Through security log monitoring and audit log monitoring, HUAWEI CLOUD provides early warning and tracking of all information security incidents, their progress, disposal measures and implementation, and analyzes the impact of incident disposal. For the daily diversified attack alarm incidents, HUAWEI CLOUD has a professional security incident management system to track the

Purposes	Brief Introduction of Controls	Measures Taken by HUAWEI CLOUD
	E.1.2 Ensure Proper Protection (Sensitive Data)	security incidents end-to-end, and the whole disposal process can be traced back.
	E.1.3 Detecting Possible Security Incidents	HUAWEI CLOUD uses IPS intrusion prevention system, web application firewall, anti-virus software and HIDS host based intrusion detection system for vulnerability management of system components and networks. IPS intrusion prevention system can detect and prevent potential network intrusion activities; Web application firewall is deployed at the network boundary to protect the security of application software from external SQL injection, CSS, CSRF and other application oriented attacks; antivirus software provides virus protection and firewall in Windows system; HIDS host type intrusion detection system protects the security of cloud server, provides weak password detection, malicious program detection, double factor authentication, vulnerability management, webpage tamper prevention and other functions. HUAWEI CLOUD continuously tracks the effectiveness of security control measures and system security configuration by combining internal and external audit.
	E.1.4 Ensure Efficient and Lasting Measures (Sensitive Data)	HUAWEI CLOUD has designed a unified analysis and early warning platform for customers to understand the overall data security posture, quickly identify and respond to security events, and perform risk assessment and security posture prediction by analyzing correlations among alarms, events, and assets. In this way, protection policies can be generated in advance to prevent potential risks.

- Data Deletion

Purposes	Brief Introduction of Controls	Measures Taken by HUAWEI CLOUD
F.1 Data Deletion	F.1.1 Establish a Data Deletion Process	HUAWEI CLOUD supports the secure deletion of data according to customer requirements. The methods of secure deletion include deleting the encryption key of encrypted storage, recycling and rewriting the underlying storage, degaussing/bending/crushing of scrapped physical media.
	F.1.2 Establish Secure Deletion Methods	HUAWEI CLOUD has established a data security processing mechanism, which specifies the requirements for the secure destruction and disposal of data. Personal data which is no longer needed will be conducted with safe disposal such as anonymization or deletion, and the corresponding records will be saved and stored. According to ISO27001 standard, the information asset classification of HUAWEI CLOUD is monitored and managed by special tools to form an asset list. Each asset is designated to an owner, and the corresponding deletion record will be formed for the deleted media or data assets.
	F.1.3 Appoint a Responsible Person for Data Deletion	
	F.1.4 Monitor the Deletion Process	HUAWEI CLOUD establishes management methods for information system security and personal data processing monitoring, and monitors and records the information security management system, data access, modification, and destruction operations for processing personal data.
	F.1.5 Discard of Media Devices (Sensitive Data)	HUAWEI CLOUD supports the secure deletion of data according to customer requirements. The methods of secure deletion include deleting the encryption key of encrypted storage, recycling and rewriting the underlying storage, degaussing/bending/crushing of scrapped physical media.

- Security Incidents

Purposes	Brief Introduction of Controls	Measures Taken by HUAWEI CLOUD
G.1 Notification of Security Incidents	G.1.1 Define Responsibilities and Procedures	HUAWEI CLOUD has established comprehensive security log management requirements, security event rating and handling processes, a 24/7 professional security event response team, and a corresponding security expert resource pool. HUAWEI CLOUD strives to achieve rapid security incident response in terms of incident detection, impact scoping, damage isolation, and service recovery. In addition, HUAWEI CLOUD keeps security event rating criteria, time to response, and time to resolution up to date by taking into account the impact of a security event or incident on our entire network and customers. Refer to the ***"HUAWEI CLOUD Security White Paper"*** published by HUAWEI CLOUD for details. When a security incident occurs, the scope, nature, personal data types affected will be summarized as reports by a HUAWEI CLOUD specialist, who shall notify the related the AAPI security incident response organizations and affected data owners as required.
	G.1.2 Prepare Reports	
	G.1.3 Notification	

- Development Environment

Purposes	Brief Introduction of Controls	Measures Taken by HUAWEI CLOUD
H.1 Security of Development Environment	H.1.1 Implement a Secure Development Policy	HUAWEI CLOUD uses DevOps and DevSecOps mode for development, realizes the separation of development, test and QA environment, and formulates corresponding management system and process to control development and change activities. HUAWEI CLOUD and related cloud services comply with security and privacy design principles and specifications as well as legal and regulation requirements. HUAWEI CLOUD runs threat analysis based on the service scenario, data flow diagram, networking model during the security requirement analysis and design phases, and specifies the threat reduction schemes. At the same time, all cloud services need to pass multiple rounds of security testing and code review before released.

5 How HUAWEI CLOUD Supports Customers to Comply with PDPL

5.1 Customers' Privacy Protection Responsibilities Under PDPL

When the customer's content data contains personal data of other data owners, the customer may be subject to the PDPL. If so, customers should comply with the requirements stipulated in the PDPL for data users, and HUAWEI CLOUD helps customers respond to their requirements and obligations as much as possible.

Core Requirements of PDPL	Customer's Privacy Protection Responsibilities	HUAWEI CLOUD Service Support Provided To Customers
Ensure the Quality of Personal Data	Customers are responsible for the quality of the personal data they collect to meet the following requirements: **Purpose Appropriateness:** Personal data collected and processed must be processed for defined, appropriate, and related purposes. **Legal and legitimate :** Data collection shall not be conducted by means of unfaithful or fraudulent means or in violation of PDPL regulations. **Purpose Restriction:** Personal data collected and processed must not be used for purposes inconsistent with or beyond the scope of collection. **Data Accuracy:** Data should be accurate and updated when necessary. **Data Correction:** For all inaccurate or incomplete data, the data user shall disable/delete or replace it after receiving the information. **Data Access:** Data users should ensure that data owners have access to personal data that they are collecting or processing. **Data Retention Restrictions:** Once no longer needed or irrelevant to the purpose of collection, the data should be destroyed.	HUAWEI CLOUD only process data in accordance with customer's instructions. Customers should collect personal data through the principle of fairness and transparency and ensure the appropriateness of the purpose. They should not use personal data for non-contractual purposes. Customers can revise and extract their own personal data stored in the HUAWEI CLOUD.When personal data is no longer needed, customers can delete it by their own. At the same time, HUAWEI CLOUD has set up a dedicated team to support and communicate with customers. When customers encounter difficulties, they can seek help from HUAWEI CLOUD through the worksheet service.

Core Requirements of PDPL	Customer's Privacy Protection Responsibilities	HUAWEI CLOUD Service Support Provided To Customers
Notifying and Obtaining Consent	Customers should ensure that notifications and consents to collect personal data comply with applicable laws and regulations: **Notifications:** When collecting personal data, the data owner should be informed in advance of the purpose of data processing, the identity of the data recipient, the consequences of inaccurate or inaccurate data provision, and the rights of the data owner in a clear and clear manner. **Explicit Consent:** A notification must be presented to the data owner in writing or other equivalent manner, either explicitly or prominently, with the consent of the data owner before data can be collected and processed.	HUAWEI CLOUD only process data in accordance with customer's instructions. The purpose and scope of content data collection are managed by the customers themselves. Some of HUAWEI CLOUD's products and services provide customers with the ability to embed privacy statements and record related operations to help them implement policies that inform their data owners about personal data processing.
Conditional Collection and Processing of Sensitive and Medical Data	Customers should determine whether sensitive personal or medical data can be collected based on their business nature. Individuals or entities that can legally collect or process sensitive or medical data should obtain the consent of their customers and use certain techniques to separate or desensitize sensitive data before storing it.	HUAWEI CLOUD products provide dynamic data desensitization and sensitive data discovery strategies to help customers generate desensitization rules and audit rules to desensitize the personal sensitive data processed and the personal sensitive data that may be contained in the processed records.

Core Requirements of PDPL	Customer's Privacy Protection Responsibilities	HUAWEI CLOUD Service Support Provided To Customers
Ensuring Data Security	Customers are required to take the necessary technical and organizational measures to ensure the security and confidentiality of personal data, to protect their personal data from changes, loss, unauthorized access or processing.	HUAWEI CLOUD provides customers with a variety of security products and services, including network security protection, incident monitoring and response, access control, data encryption and other products. See chapter 5.3 of this document for details. HUAWEI CLOUD provides special security products to help customers improve their security capabilities in some aspects, such as Database Security Service, **Advanced Anti-DDoS (AAD)**, **Vulnerability Scanning Service**, etc.
Confidentiality Obligations	Customers and all personel who participate in any stage of personal data processing are obligated to keep personal data confidential. Even if they are no longer data users or participants in personal data processing, they still have a duty of confidentiality.	HUAWEI CLOUD's employees have signed a confidentiality agreement, which stipulates their confidentiality obligations in data processing, and periodically audits their compliance.
Consent for Data Transfer	Before transmitting personal data, the customer should provide the data owner with information about the purpose of the transfer, the relevant personal data category, and the nature of the data sharing, and obtain the consent of the data owner for the transfer.	Some of HUAWEI CLOUD products and services provide clients with an interface to embed privacy statements and the ability to record related operations. Customers can inform data owners in the privacy statements about the purpose of transfer, related personal data categories, and nature of data sharing.

Core Requirements of PDPL	Customer's Privacy Protection Responsibilities	HUAWEI CLOUD Service Support Provided To Customers
Conditional Cross-Border Transfer	Customers should conduct cross-border transfer of personal data only when they confirm that the data transfer are made to country that have an adequate level of data protection.	Some of HUAWEI CLOUD products and services provide clients with the ability to embed privacy statements and record related operations. Customers can notify data owners in their privacy statements that their personal data may be transmitted and stored in other countries and regions.
Data Registration Requirements	Before processing content data, customers should register relevant information with a registry established by the local regulatory body, including the name and address of the person in charge, the purpose of collecting personal data, the nature of collecting personal data, the method of collecting and updating personal data, the means of ensuring data security, and the possible destination for transmitting personal data.	-
Time Limitation of Data Retention	After fulfilling the contractual obligations, the stored personal data should be deleted in time. Personal data can be retained for a maximum of 2 years, given reasonable speculation about possible future services	Customers should form the deletion mechanism of personal data in content data and can delete specified data through cloud database products.

Core Requirements of PDPL	Customer's Privacy Protection Responsibilities	HUAWEI CLOUD Service Support Provided To Customers
Data Processing Limitations for Direct Marketing	Customers can send business information for E-marketing to data owners only under specific circumstances, such as when personal data is available in public documents, data owners provide it on their own initiative, and data users agree to it.	Some of HUAWEI CLOUD products and services provide clients with the ability to embed privacy statements and record related operations. Customers can inform data owners in the privacy statement that their personal data will be used for marketing purposes.

5.2 Customer's Compliance Responsibilities with Resolution 47/2018

As a data user, customer should improve data security measures in accordance with the requirements of Resolution 47/2018.

PURPOSE	BRIEF INTRODUCTION OF CONTROLS	Data Security Responsibility
A. Data Collection		
A.1 Integrity	A.1.1 To Ensure Data Completeness	**Customer's Privacy Responsibility:** As a data user, customers should ensure the integrity of the collected personal data during transfer and adopt appropriate encryption methods to protect personal data during transfer. Customers should ensure the accuracy of personal data collection and data validation of data provided by data owners. Customers should set up access control and identity management to restrict unauthorized access to the collected personal data. **HUAWEI CLOUD Provides Customer Service Support:** HUAWEI CLOUD Products provides security products and
	A.1.2 To Minimization Uploading Mistakes	
	A.1.3 To Ensure Data Integrity	
A.2 Confidentiality	A.2.1 To Warrant Confidentiality During the Entire Data Collection Process	
	A.2.2 To Restrict Access to Data Collection	

PURPOSE	BRIEF INTRODUCTION OF CONTROLS	Data Security Responsibility
	A.2.3 To Restrict Unauthorized Access During Collection	services such as Identity and Access Management (IAM), Direct Connect (DC), Virtual Private Network (VPN), and Data Encryption Workshop (DEW) to help customers ensure confidentiality and access control during personal data collection and avoid the risk of unauthorized access.
B. Access Control		
B.1 Identification of Assets	B.1.1 Identify Assets	**Customer's Privacy Responsibility:** As a data user, the customer should identify the personal data assets being processed, form a list of responding data assets, and confirm with the owner of the assets. Customers should set up access control and authentication mechanisms for personal data and systems that process personal data, encrypt systems and personal data that process personal data, assign corresponding access rights, and prevent unauthorized access to system or personal data. And customers should monitor the system and open access logs to record and monitor the activities of system users accessing personal data. **HUAWEI CLOUD Provides Customer Service Support:** The Elastic Cloud Server (ECS) products provided by HUAWEI CLOUD to customers includes the ability to tag cloud resources such as instances, mirrors, and disks. If there are multiple cloud resources under the customer's account, and there are multiple associations between different cloud resources, the cloud resources
	B.1.2 Identify Responsible Parties and Determine Their Responsibilities	
	B.1.3 Verify the Controls Application	
B.2 Access of Data	B.2.1 Manage Access to Systems	
	B.2.2 Assign Permission	
	B.2.3 Verify the Identification and the Authorization	
	B.2.4 Control Physical Access to Data Centers	
	B.2.5 Monitoring Activities	

PURPOSE	BRIEF INTRODUCTION OF CONTROLS	Data Security Responsibility
	B.2.5 Monitoring Activities (Sensitive data)	can be tagged to realize the classification and unified management of cloud resources, so that the customer can identify and manage information assets. In addition, HUAWEI CLOUD's IAM services can manage employee privileges by role and validate employee identities through multifactor validation. Also, the IAM collaborates with Log Tank Service (LTS) and Cloud Trace Service (CTS) to record and audit the operations of employees and monitor the occurrence of abnormal behavior.
C. Change Control		
C.1 Change Control	C.1.1 Ensure Changes	**Customer's Privacy Responsibility:** Customers should verify the maintenance of the production environment and protect the integrity of their personal data during changes to the production environment. Production environments should be isolated with set-up access controls. Customers should also ensure that the integrity, availability, and confidentiality of personal data are verified and any records are maintained. **HUAWEI CLOUD Provides Customer Service Support:** Customers can use the Host Security Service (HSS) to check the integrity of the mirrored file, compare it to determine if the current file state is different from its state when the file was last scanned, and use this comparison to determine whether valid or suspect modifications have occurred to the file. When potential risks

PURPOSE	BRIEF INTRODUCTION OF CONTROLS	Data Security Responsibility
	C.1.1 Ensure Changes (Sensitive Data)	are discovered, the customer will be promptly reminded.
D. Backup and Recovery		
D.1 Backup Copies and Recovery Procedure	D.1.1 Ensure a Formal Backup and Recovery Procedure	**Customer's Privacy Responsibility:** Customers should set up appropriate backup policies and backup recovery processes, encrypt backup copies, and set up access control measures to protect the security of backups. **HUAWEI CLOUD Provides Customer Service Support:** HUAWEI CLOUD provides customers with Cloud Backup and Recovery (CBR), Volume Backup Service (VBS), and Cloud Server Backup Service (CSBS). Customers can back up data and servers as needed and set access authorization of backed up data through IAM.
	D.1.2 Ensure Access Control	
	D.1.2 Ensure Access Control (Sensitive Data)	
E. Vulnerability Management		
E.1 Vulnerability Management	E.1.1 Prevent Security Incidents by Design	**Customer's Privacy Responsibility:** Customers should establish a sound security incident management mechanism to prevent and monitor the occurrence of security incidents. Customers should prevent and monitor security incidents through vulnerability scanning, environmental isolation, foreign intrusion protection, audit logs, and ongoing device/hardware/program updates. **HUAWEI CLOUD Provides Customer Service Support:** HUAWEI CLOUD has a dedicated Product Security Incident Response Team to help customers establish a mature vulnerability response
	E.1.2 Ensure Proper Protection	
	E.1.2 Ensure Proper Protection (Sensitive Data)	
	E.1.3 Detecting Possible Security Incidents	

PURPOSE	BRIEF INTRODUCTION OF CONTROLS	Data Security Responsibility
	E.1.4 Ensure Efficient and Lasting Measures (Sensitive Data)	mechanism to reduce the risk of vulnerabilities. At the same time, customers can also use the five core functions of the Vulnerability Scanning Service (VSS) provided by HUAWEI CLOUD to discover security risks exposed by websites or servers in the network automatically. The five core functions are web vulnerability scanning, operating system vulnerability scanning, asset content compliance detection, configuration baseline scanning, and weak password detection HUAWEI CLOUD provides Host Security Service (HSS) to provide the functions of asset management, vulnerability management, baseline inspection, intrusion detection, etc. to reduce host security risks and enhance overall security assurance capabilities.
F. Data Deletion		
F.1 Data Deletion	F.1.1 Establish a Data Deletion Process	**Customer's Privacy Responsibility:** Customers should set up a data destruction mechanism to delete personal data when the data owner requests or the data user no longer needs it, to ensure the security, confidentiality and irreversibility of the destruction, and to keep the corresponding records of the destruction. Customers should set up destruction mechanisms for media that store personal data and implement physical destruction processes through demagnetization, decomposition, incineration,
	F.1.2 Establish Secure Deletion Methods	
	F.1.3 Appoint a Responsible Person for Data Deletion	
	F.1.4 Monitor the Deletion Process	

PURPOSE	BRIEF INTRODUCTION OF CONTROLS	Data Security Responsibility
	F.1.5 Discard of Media Devices (Sensitive Data)	and shredding or replication technologies. **HUAWEI CLOUD Provides Customer Service Support:** HUAWEI CLOUD only follows the customer's instructions for data destruction. The type, quantity and media of data destroyed are at the customer's discretion.
G. Security Incidents		
G.1 Notification of Security Incidents	G.1.1 Define Responsibilities and Procedures	**Customer's Privacy Responsibility:** Customers should establish a sound reporting mechanism for security incidents, and quickly form and report security incidents to related parties after the occurrence of security incidents. **HUAWEI CLOUD Provides Customer Service Support:** Customers can use the Cloud Eye Service (CES) to monitor the running status of the server and the resources on the cloud in real time. When a hardware failure occurs, CES will notify the customer via email, SMS, and HTTP/S.
	G.1.2 Prepare Reports	
	G.1.3 Notification	
H. Development Environment		

PURPOSE	BRIEF INTRODUCTION OF CONTROLS	Data Security Responsibility
H.1 Security of Development Environment	H.1.1 Implement a Secure Development Policy	**Customer's Privacy Responsibility:** Customers should be responsible for formulating and implementing security development strategies to meet the security requirements for the development environment as defined by regulations. Customers should also encrypt or anonymize personal data in their development environment. **HUAWEI CLOUD Provides Customer Service Support:** HUAWEI CLOUD supports customers to establish isolated production and testing environment processes in the cloud using Virtual Private Cloud VPC.

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

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

- **Management and Deployment of Products**

Product	Description	Corresponding Core Requirements and Control Measures
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.	PDPL - Ensure the quality of personal data PDPL - Ensure data security; PDPL-Confidentiality Obligation; Resolution 47/2018-A.2; Resolution 47/2018-B.1; Resolution 47/2018-B.2;
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.	PDPL - Ensure data security; PDPL-Confidentiality Obligation; Resolution 47/2018-A.2; Resolution 47/2018-B.1; Resolution 47/2018-B.2;
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.	PDPL - Ensure the quality of personal data PDPL - Ensure data security; Resolution 47/2018-E.1; Resolution 47/2018-G.1;

Product	Description	Corresponding Core Requirements and Control Measures
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 requirements. Customers can keep records of operations on personal data through LTS to guarantee the data owners' right to know.	PDPL - Ensure data security; PDPL-Confidentiality Obligation; Resolution 47/2018-A.2; Resolution 47/2018-B.1; Resolution 47/2018-B.2; Resolution 47/2018-G.1;

- **Security Products**

Product	Description	Corresponding Privacy Protection Obligations
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.	PDPL - Ensure the quality of personal data PDPL - Ensure data security; Resolution 47/2018-A.1; Resolution 47/2018-E.1; Resolution 47/2018-G.1;

Product	Description	Corresponding Privacy Protection Obligations
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.	PDPL - Ensure the quality of personal data PDPL - Ensure data security; Resolution 47/2018-A.1; Resolution 47/2018-A.2; Resolution 47/2018-E.1;
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.	PDPL - Ensure the quality of personal data PDPL - Ensure data security; Resolution 47/2018-A.1; Resolution 47/2018-E.1; Resolution 47/2018-G.1;

Product	Description	Corresponding Privacy Protection Obligations
Vulnerability Scan Service (VSS)	Vulnerability Scan Service (VSS) is a multi-dimensional security detection service, with five core functions: web vulnerability scanning, asset content compliance detection, configuration baseline scanning, operating system vulnerability scanning, and identification of systems with a weak password. VSS enables customers to protect their data integrity by automatically identifying security threats on their exposed websites or servers.	PDPL - Ensure the quality of personal data PDPL - Ensure data security; Resolution 47/2018-A.1; Resolution 47/2018-E.1; Resolution 47/2018-G.1;
Advanced Anti-DDoS (AAD)	Advanced Anti-DDoS (AAD) is a value-added security defense service that defends against large volumetric DDoS attacks on Internet servers. Customers can configure AAD to divert the attack traffic to high-defense IP addresses with significant defense capabilities for scrubbing, keeping customers' business stable and reliable.	PDPL - Ensure the quality of personal data PDPL - Ensure data security; Resolution 47/2018-A.1; Resolution 47/2018-E.1; Resolution 47/2018-G.1;

- **Network Products**

Product	Description	Corresponding Privacy Protection Obligations
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.	PDPL - Ensure the quality of personal data PDPL - Ensure data security; Resolution 47/2018-A.1; Resolution 47/2018-A.2; Resolution 47/2018-E.1;

Product	Description	Corresponding Privacy Protection Obligations
Virtual Private Cloud (VPC)	Virtual Private Cloud (VPC) enables customers to create private, isolated virtual networks on HUAWEI CLOUD. Customers can configure IP address ranges, subnets, and security groups, assign Elastic IP (EIP) addresses, and allocate bandwidth in a VPC. VPC is the customer's private network on the cloud, with 100% isolation from other customers, enhancing the data security on the cloud.	PDPL - Ensure the quality of personal data PDPL - Ensure data security; Resolution 47/2018-A.1; Resolution 47/2018-A.2; Resolution 47/2018-B.1; Resolution 47/2018-B.2; Resolution 47/2018-H.1;

- **Storage Products**

Product	Description	Corresponding privacy protection obligations
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 reliability, and reduce the risk of data tampering.	PDPL - Ensure the quality of personal data PDPL - Ensure data security; Resolution 47/2018-D.1;

Product	Description	Corresponding privacy protection obligations
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.	PDPL - Ensure the quality of personal data PDPL - Ensure data security; Resolution 47/2018-D.1;

6 HUAWEI CLOUD Privacy Protection Related Certifications

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

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

Privacy Related Standard Certifications:

- **ISO 27701**

  Privacy information management system certification. The ISO 27701 certification shows that HUAWEI CLOUD has established a solid management system related to data privacy protection.

- **ISO 29151**

  International practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.

- **ISO 27018**

  International code of conduct focused on the protection of personal data in Cloud. The adoption of ISO 27018 indicates that HUAWEI CLOUD has met the requirements of an internationally recognized personal data protection measures of public cloud platform, and can guarantee the security of customers' personal data.

- **BS 10012**

  Personal data management system standard issued by the British Standards Institute (BSI). The BS 10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.

- **SOC2 Audit**

An independent audit report issued by a third party audit institution based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers. At present, HUAWEI CLOUD has passed the audit of SOC2 type 1 Privacy Principle, which proves that HUAWEI CLOUD has reasonable control measures in terms of cloud management and technology.

Data Security Standard Certifications:

- ISO 27001 Information Security Management System Certification
- ISO 27017 Cloud Service Information Security Management System
- ISO 20000 Information Technology Service Management System Certification
- ISO 22301 Business Continuity Management System
- ISO 27799 Health Information Security Management System Certification
- CSA STAR Cloud Security International Gold Certification
- PCI DSS Third-Party Payment Industry Data Security Standard Certification
- International Common Criteria (CC) EAL3+ Security Assessment Standard
- Management & Operations Stamp of Approval (M&O Program)
- NIST Cybersecurity Framework
- Payment Card Industry Three Domain Secure Certification (PCI 3DS)

Regional Security Certifications:

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

7 Conclusion

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

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

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

This white paper is for reference only and does not have any legal effect or constitutes a legal advice. Customers should assess their own situation when using cloud services and ensure compliance with the PDPL and other regulatory requirements when using HUAWEI CLOUD.

8 Version History

Date	Version	Description
December 2020	1.0	First release

