HUAWEI CLOUD Compliance with Mexican Privacy Protection Laws and Regulations

Issue 1.1

Date 2024-08-05

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
1.1 Scope of Application 1
1.2 Purpose of Publication 1
1.3 Basic Definitions 1
2 Privacy Protection Responsibilities 3
3 Overview of Mexican Privacy Protection Laws and Regulations 5
3.1 Background of Mexican Privacy Protection Laws and Regulations 5
3.2 HUAWEI CLOUD's Role under Mexican Privacy Protection Laws and Regulations 5
4 How HUAWEI CLOUD is Satisfying the Requirements of Mexican Privacy Protection Laws and Regulations 7
4.1 HUAWEI CLOUD Privacy Commitment 7
4.2 HUAWEI CLOUD Basic Privacy Protection Principles 7
4.3 HUAWEI CLOUD’s Compliance Measures in Response to the Federal Law on the Protection of Personal Data held by Private Parties and its Regulations 8
4.4 HUAWEI CLOUD’s Compliance Measures in Response to the General Law for the Protection of Personal Data in Possession of Obligated Subjects 23
5 How HUAWEI CLOUD Supports Customers to Comply with Mexican Privacy Protection Laws and Regulations 26
5.1 Customer's Privacy Protection Responsibilities under the Federal Law on the Protection of Personal Data held by Private Parties and its Regulations 26
5.2 Customer's Privacy Protection Responsibilities under the General Law for the Protection of Personal Data in Possession of Obligated Subjects 39
5.3 How HUAWEI CLOUD Products and Services Help Customers Implementing Content Data Privacy and Security 53
6 HUAWEI CLOUD Privacy Protection Related Certifications 60
7 Conclusion 62
8 Version History 63

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 United Mexican States ("Mexico").

1.2 Purpose of Publication

This document is intended to help customers understand:

- HUAWEI CLOUD's privacy protection responsibility model;
- Mexican privacy laws and regulations;
- HUAWEI CLOUD's responsibilities on compliance with Mexican privacy laws and regulations;
- HUAWEI CLOUD's controls and achievements in privacy management;
- Customers' responsibilities and obligations when falling under Mexican privacy laws and regulations jurisdiction, as specified in the responsibility model;
- How to leverage HUAWEI CLOUD's security products and services to achieve privacy compliance.

1.3 Basic Definitions

- **Personal Data**

  Any information concerning an identified or identifiable natural person. A person is considered identifiable when his/her identity can be determined directly or indirectly through any information.

- **Sensitive Personal Data**

  Data that refers to the most intimate sphere of its owner, or whose improper use may give rise to discrimination or entail a serious risk for the owner. By way of example, but not limited to, personal data that may reveal aspects such as racial or ethnic origin, present or future health status, genetic information, religious, philosophical and moral beliefs, political opinions and sexual preference are considered sensitive.

- **Data Controller**

  - Individual or private legal entity that decides on the processing of personal data. (Definition in the Federal Law on the Protection of Personal Data held by Private Parties)
  - The regulated entities decide on the processing of personal data including any authority, entity, organ and body of the Executive, Legislative and Judicial Branches, autonomous bodies, political parties, trusts and public funds. (Definition in the General Law for the Protection of Personal Data in Possession of Obligated Subjects)
- **Data Processor**
  - The individual or legal entity that, alone or jointly with others, processes personal data on behalf of the data controller. (Definition in the Federal Law on the Protection of Personal Data held by Private Parties)
  - The natural person or public or private legal entity, outside the organization of the Controller, who alone or jointly with others processes personal data in the name and on behalf of the Controller. (Definition in the General Law for the Protection of Personal Data in Possession of Obligated Subjects)
- **Data Subject**

  The natural person to whom the personal data corresponds.
- **ARCO Rights**

  The rights of access, rectification, cancellation and opposition to the processing of personal data.
- **Cancellation**

  The data controller stops processing personal data. The cancellation of personal data will lead to a blocking period.
- **Blocking**

  The identification and conservation of personal data once the purpose for which they were collected has been fulfilled, for the sole purpose of determining possible liabilities in relation to their processing, until the legal or contractual statute of limitations period. During such period, personal data may not be subject to processing and after such period, it will be cancelled in the corresponding database.
- **Suppression**

  Activity consisting in eliminating, erasing, or destroying personal data, once the blocking period has elapsed, under security measures previously established by a data controller.
- **HUAWEI CLOUD**

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

  Registered users having a business relationship with HUAWEI CLOUD.
- **Account Information**

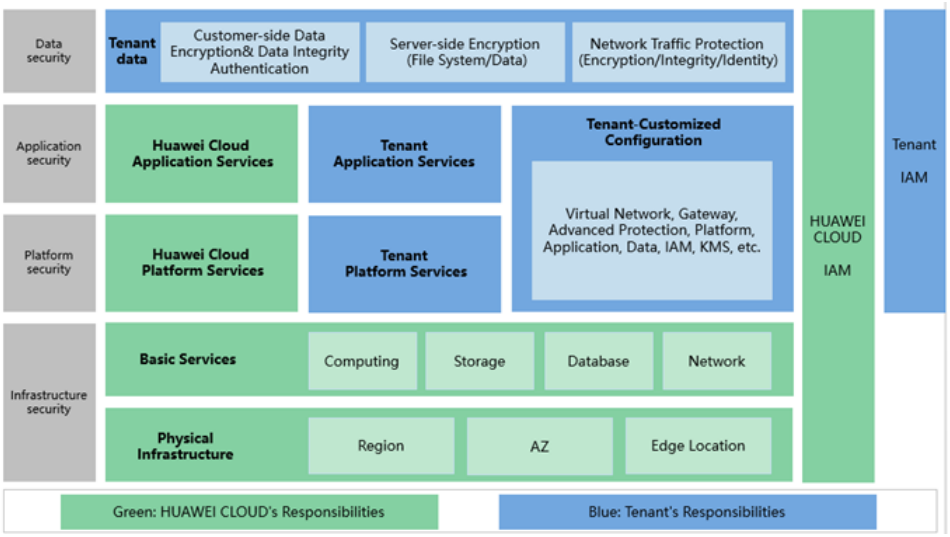
  Personal data, such as names, phone numbers, email addresses, bank accounts and billing information provided by customers to HUAWEI CLOUD when creating or managing their HUAWEI CLOUD accounts. HUAWEI CLOUD acts as the data controller of any personal data included within account information.
- **Content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

  Data stored or processed during the use of HUAWEI CLOUD services, including but not limited to documents, software, images, and audio and video files.

2 Privacy Protection Responsibilities

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

Figure 2-1 Responsibility Sharing Model



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

HUAWEI CLOUD: As the Cloud Service Provider (CSP), HUAWEI CLOUD is not only responsible for the security and compliance of personal data collected or processed during business operations, but also for the platform security defined by the security and compliance of HUAWEI CLOUD's infrastructure, including the cloud platform and software applications offered to tenants.

- **Protection of Tenant Privacy**: HUAWEI CLOUD identifies and protects tenants' personal data. HUAWEI CLOUD's policy, processes and operations not only resulted in the formulation of privacy protection policies but also in the deployment of active privacy control measures, such as anonymization, data encryption, system and platform security protections, all helping to ensure the security of tenants' personal data.

- **Platform and Tenant Security Support**: HUAWEI CLOUD is responsible for the security and compliance of the platform and infrastructure included in the cloud service, ensuring the platform and applications' security levels comply with the requirements of applicable privacy protection laws and regulations.

  At the same time, HUAWEI CLOUD provides tenants with a variety of privacy protection technologies and services in order to help tenants protect their privacy, such as access control, authentication, data encryption, logging and auditing functions, in order to help tenants protect their privacy according to their commercial requirements.

  Tenant: As purchaser of HUAWEI CLOUD's products and services, tenants are free to decide on how to use them to store or process content data, which may include personal data. Therefore, tenants are responsible of Content Security, which is defined as the security and compliance of content data.
- **Content Data Protection:** Tenants should correctly and comprehensively identify personal data in the cloud, formulate policies to protect data security and privacy, and finally select appropriate privacy protection measures. Specific measures shall include security configuration based on business and privacy protection requirements, such as operating system configuration, network settings, security protection, database encryption, policy configuration and set appropriate access controls and password policies.
- **Respond to data subject requests**: Tenants shall guarantee the rights of data subjects and respond to their requests in a timely manner. In the case of a personal data breach, the tenant shall notify both regulatory authorities and data subjects, and take adequate actions in accordance with regulatory requirements.

3 Overview of Mexican Privacy Protection Laws and Regulations

3.1 Background of Mexican Privacy Protection Laws and Regulations

In 2009, the protection of personal data was recognized as a fundamental right in an amendment to the Mexican Constitution. Immediately thereafter, Congress enacted the Federal Law on the Protection of Personal Data held by Private Parties (the "Private Data Protection Law"), which entered into force on July 6, 2010. The Private Data Protection Law is comprehensive and sets out the principles and minimum standards to be followed by all private subjects in the processing of any personal data. Subsequently, on December 22, 2011, the Regulation of the Federal Law on the Protection of Personal Data held by Private Parties was issued, which aims to clarify the scope of the principles and obligations set forth in the Private Data Protection Law.

The General Law for the Protection of Personal Data in Possession of Obligated Subjects (the "Obligated Subjects Data Protection Law") was enacted on January 27, 2017. The Obligated Subjects Data Protection Law establishes the legal framework for the protection of personal data by, at the federal, state and municipal levels, any authority, entity, organ and body of the Executive, Legislative and Judicial Branches, autonomous bodies, political parties, trusts and public funds.

3.2 HUAWEI CLOUD's Role under Mexican Privacy Protection Laws and Regulations

The main difference between the above-mentioned Mexican privacy laws and regulations is that the regulated subjects are different. The Private Data Protection Law and its regulations apply to private subjects that process personal data, including individuals and private legal entities. The Obligated Subjects Data Protection Law applies to any authority, entity, organ and body of the Executive, Legislative and Judicial Branches, autonomous bodies, political parties, trusts and public funds. The activity regulated by laws is any processing of personal data in physical or electronic media, regardless of the form or method of its creation, type of media, processing, storage or organization.

HUAWEI CLOUD, as a legal entity providing public cloud services in Mexico, qualifies as a private subject as defined in the Private Data Protection Law and needs to follow the

requirements in the Private Data Protection Law and its regulations. Also, according to the obligations of data processors as defined in the Obligated Subjects Data Protection Law, when HUAWEI CLOUD's customers are obligated subjects, HUAWEI CLOUD needs to follow the requirements of the Obligated Subjects Data Protection Law for data processors.

Personal data processed by HUAWEI CLOUD mainly includes customers' content data and personal data provided by customers when performing operations on HUAWEI CLOUD platform, including but not limited to registering, purchasing services, real-name authentication and service support. As customers have full control over their content data, when processing personal data included in content data, HUAWEI CLOUD is generally regarded as the data processor. HUAWEI CLOUD acts as the data controller when dealing with personal data provided by the customers' set up or management of their HUAWEI CLOUD account.

HUAWEI CLOUD acts as the data controller of customers' personal data: When a customer performs operations on HUAWEI CLOUD platform, including but not limited to registering, purchasing services, real-name authentication and service support, HUAWEI CLOUD will collect some personal data, such as the customer's name, address, ID number, bank accounts, and other types of information according to the service used. HUAWEI CLOUD is ultimately responsible for the security and privacy protection of such customers' personal data, ensuring that the collection, processing and storage procedures comply with legal requirements, responding to data subjects' requests, complying with the requirements of Mexican privacy protection laws and regulations regarding limited disclosure, and finally taking actions to avoid data breaches.

HUAWEI CLOUD acts as the data processor of customer's content data: When customers use HUAWEI CLOUD services or applications on behalf of a controller to process personal data included in their content, HUAWEI CLOUD is the data processor. HUAWEI CLOUD processes personal data on behalf of customers in accordance with personal data processing requirements or instructions from the data controller, and maintains records of data processing operations.

4 How HUAWEI CLOUD is Satisfying the Requirements of Mexican Privacy Protection Laws and Regulations

4.1 HUAWEI CLOUD Privacy Commitment

HUAWEI CLOUD has fully integrated cyber security and privacy protection into each cloud service providing and promising to provide customers with stable, reliable, secure, trustworthy, and evolvable services while respecting and protecting customers' privacy.

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

4.2 HUAWEI CLOUD Basic Privacy Protection Principles

- **Lawfulness, Fairness and Transparency**

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

- **Purpose Limitation**

  HUAWEI CLOUD collects personal data for 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 subjects.

- **Accuracy**

  HUAWEI CLOUD ensures that personal data is accurate and, when necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay depending on the purpose of data processing.

- **Storage Limitation**

  Personal data will not be kept beyond the period necessary for the purposes of data processing.

- **Integrity and Confidentiality**

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

- **Accountability**

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

4.3 HUAWEI CLOUD's Compliance Measures in Response to the Federal Law on the Protection of Personal Data held by Private Parties and its Regulations

Based on the characteristics of HUAWEI CLOUD's business and in accordance with the requirements of the Private Data Protection Law and its regulations, HUAWEI CLOUD, as a legal entity that processes personal data, assumes the roles of both data controller and data processor in different scenarios. HUAWEI CLOUD actively responds and fulfills its obligations by adopting the following privacy protection mechanisms and technologies to comply with the requirements of the Private Data Protection Law. The following specific requirements applied by HUAWEI CLOUD incorporate the requirements of the Private Data Protection Law, which is supplemented by the requirements of the regulations.

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
Measures to comply with the principles of personal data processing	HUAWEI CLOUD must comply with the principles of legality, consent, notice, quality, purpose, fidelity, proportionality, and accountability under the law. To achieve this, HUAWEI CLOUD can use standards, best international practices, corporate policies, self-regulation arrangements, or any other mechanism that it determines is adequate for such purpose. Measures include at least: I. Prepare privacy policies and programs that are binding and enforceable within HUAWEI CLOUD. II. Implement a program of training, updating, and raising the awareness of personnel about	HUAWEI CLOUD has established a Privacy Information Management System (PIMS) for organization-wide privacy management in accordance with ISO 27701 international standard requirements, implementing documented privacy policies and procedures to provide guidance for personal data processing. HUAWEI CLOUD reviews the information security and privacy information management system documentation at least once a year and updates it as needed to reflect changes in business objectives or risk environments. Changes to information security and privacy policies and procedures require senior management approval.

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
	protecting personal data. III. Establish an internal supervision and monitoring systems, as well as external inspections or audits to verify compliance with privacy policies. IV. Dedicated resources for the implementation of privacy programs and policies. V. Implement a procedure to deal with the risk to the protection of personal data by the implementation of new products, services, technologies and business models, as well as to mitigate them. VI. Periodically review the security policies and programs to determine modifications required. VII. Establish procedures to receive and respond the questions and complaints of data subjects. VIII. Have mechanisms to comply with privacy policies and programs, as well as sanctions for a breach thereof. IX. Establish measures to protect personal data, in other words, a group of technical and administrative actions that will allow HUAWEI CLOUD to ensure compliance with the principles and obligations established by the Law and these Regulations. X. Establish measures to trace personal data, in other words, actions, measures, and technical procedures that will allow the tracing of personal data while being processed.	To effectively identify and control privacy risks, HUAWEI CLOUD carries out privacy risk analysis and management in the process of cloud service. HUAWEI CLOUD requires that Privacy Impact Assessment (PIA) be performed before personal data is processed, which mainly includes identifying personal data items involved in the business, business scenarios and the processes of processing, compliance analysis, possible impacts on data subjects, risk analysis and development of risk control measures and plans, etc. Only after privacy risks are reduced to an acceptable level can the business be conducted. For cloud services, we require a PIA to be conducted at the planning stage of cloud services, and a detailed analysis of privacy risks to be performed in the design activities and incorporate all privacy risk control requirements into the design plan. HUAWEI CLOUD has developed a top-down governance structure, with leadership making decisions and approving information security and privacy protection policies and objectives, information security and privacy protection-related roles and responsibilities, developing corresponding information security plans, allocating resources required to execute information security activities, and providing support to other roles within the system to promote continuous system improvement. HUAWEI CLOUD has established a formal and regular audit program, including continuous and independent internal and external assessments. Internal assessments continuously track the effectiveness of control measures, and external assessments are audited as

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
		independent auditors to verify the implementation and operational effectiveness of HUAWEI CLOUD's control environment. At the same time, HUAWEI CLOUD regularly conducts management reviews every year to identify problems in the operation of the system and implement corrective actions to promote continuous improvement of the management system. In terms of tracking personal data processing, HUAWEI CLOUD monitors and audits access operations of key systems through logging and auditing technologies. HUAWEI CLOUD has established its own training mechanism to design suitable training programs for employees according to different roles and positions. New employees must pass induction training and exams on information security and privacy protection before they are regularized; employees on board need to choose the appropriate courses for study and exams according to different business roles, with the training frequency for general employees being at least once a year and more frequent for employees in core positions. Managers are required to attend network security training and seminars. For security and privacy awareness, HUAWEI CLOUD conducts relevant training for all employees to help them understand the organization's information security and privacy protection policies and policies, while employees must commit to comply with the company's policies and system requirements. HUAWEI CLOUD has developed and implemented a violation policy that can be viewed and studied by all employees, and regularly organizes training to improve

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
		employees' understanding of violations, consequences of violations, and penalties. HUAWEI CLOUD provides a **unified communication interface** to the outside world, which is responsible for collecting and handling customer complaints. Any user can make service inquiries, feedback and complaints through a variety of channels. In addition to the **online customer service** and complaint suggestion hotline, customers can also **submit service tickets** to raise questions or make complaints through the HUAWEI CLOUD official website, and HUAWEI CLOUD will handle customer complaints in a timely manner according to the internally developed customer complaint handling process.
Privacy Notice	HUAWEI CLOUD shall inform the data subject, through a Privacy Notice, prior to collecting personal data, of the personal data collected from the data subject and the purposes of processing, in particular with respect to processing regarding marketing, advertising or business exploration and processing that is used for decision-making without human intervention. The Privacy Notice should also include HUAWEI CLOUD's company name and address, any transfers of personal data, and when HUAWEI CLOUD automatically obtains personal data using remote or local electronic, optical or other technical means of communication mechanisms, the use of such technology and the manner in which the data subject objects to its use. The mechanism for allowing the data subject to object to what is described in the Privacy Notice, restrictions on the use or disclosure of data and withdrawal of consent, the manner	When registering an account, the customer is provided with the **Privacy Statement** and is asked for his consent. The **Privacy Statement** includes the purpose of data processing including sending marketing information, and the processing of sensitive data and its purpose, and informs users of their data subject rights, including the right to object to processing and withdraw consent, and the way to exercise their rights. When the scope or use purpose of personal data collected by the product or service changes, the Privacy Statement will be updated accordingly, and customers will be asked again for their consent. Additional Privacy Statements will be provided in the product agreement and the customer's consent will be obtained 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

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
	in which the data subject's rights are exercised, the method of notifying the data subject of changes to the Privacy Notice, and the processing of sensitive personal data shall also be communicated through the Privacy Notice. The Privacy Notice may be provided to the data subject orally, on paper, electronically, in video or audio format, or through any other technology. The Privacy Notice must be simple and contain the necessary information in language, structure and design that is clear and easy to understand. If the personal data is not obtained directly from the data subject, HUAWEI CLOUD must notify the data subject of the changes to the Privacy Notice. In cases where it is not possible to provide the Privacy Notice to the data subject, or in cases where a disproportionate payment is made due to the excessive number of data subjects or the age of the data, HUAWEI CLOUD may submit a request to the supervisory authority (INAI, the National Institute of Transparency for Access to Information and Personal Data Protection) to implement compensatory measures using mass communication media, if authorized.	Statement. HUAWEI CLOUD collects personal data only when necessary for providing services. The purpose and manner of collection principle includes: user consent, contract enforcement, legal compliance, protection of not only organizations' legitimate interests, but also data subjects and others' key benefits.
Consent of the data subject	All processing of personal data shall be subject to the consent of the data subject. Implied consent is generally valid unless the data subject is required by law to give explicit consent. If the data subject does not object to the Privacy Notice, the data subject`s implied consent to the data processing may be deemed to be given, provided that the Privacy Notice contains sufficient information. If HUAWEI CLOUD intends to process the data for purposes other	When registering an account, the customer is provided with the **Privacy Statement** and is asked for his consent. The **Privacy Statement** includes the purpose of data processing including sending marketing information, and the processing of sensitive data and its purpose, and informs users of their data subject rights, including the right to object to processing and withdraw consent, and the way to exercise their rights. When the scope or use purpose of

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
	than those described in the Privacy Notice that are incompatible or similar, the consent of the data subject must be obtained again. The data subject may refuse or withdraw consent to the processing of the data at any time, and may object to the processing of its data for unnecessary purposes. However, refusal, withdrawal of consent or objection to processing by the data subject does not terminate the processing based on the necessary purposes and the legal relationship between HUAWEI CLOUD and the data subject.	personal data collected by the product or service changes, the Privacy Statement will be updated accordingly, and customers will be asked again for their consent. Additional Privacy Statements will be provided in the product agreement and the customer's consent will be obtained 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.
Requirements for establishing security measures	HUAWEI CLOUD must establish and maintain no less than physical and technical administrative security measures for managing information within its organization to protect personal data from damage, loss, alteration, destruction, or unauthorized use, access, or processing. Security measures may be taken by the controller itself or outsourced to individuals or legal entities. Consideration should also be given to the risks inherent in the classification of data types, the sensitivity of personal data, technological developments, the possible consequences of data breaches on data subjects, the number of data subjects involved, previous breaches in the processing system, the risks arising from the potential value of personal data to outsiders, and other factors affecting the level of risk such as those resulting from laws and regulations.	HUAWEI CLOUD has adopted strict administrative and technical controls to ensure personal data security in the access, transfer, storage, processing and other stages of personal data lifecycle. • In terms of authentication, strict password policy and multi-factor authentication are adopted; • In the aspect of permission management, role-based access control and permission management for operation and maintenance personnel is implemented; • In terms of data storage and transmission, sensitive data encryption is adopted; • In terms of data processing, monitoring and auditing of access to critical systems through logging and auditing of data processing is adopted. Customers can also verify the privacy and security controls within HUAWEI CLOUD's environment through HUAWEI CLOUD security reports or certifications obtained. HUAWEI CLOUD has obtained multiple certifications from privacy compliance related

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
		international standard, including ISO 27701, ISO 29151, ISO 27018, BS 10012, SOC, privacy audit reports (please refer to Chapter 6 for a detailed introduction of certifications) Among all the international standards, ISO27018 is the international code of conduct focusing on the protection of personal data regarding cloud, its adoption indicates that HUAWEI CLOUD has a complete personal data protection management system.
Measures taken to protect the security of personal data	In order to establish and maintain the security of personal data, HUAWEI CLOUD must take the following actions into account: I. Prepare a list of personal data and processing systems. II. Identify the responsibilities and obligations of those who process personal data. III. Identify the responsibilities and obligations of those who process personal data. IV. Conduct a risk analysis of personal data, including identification of hazards and estimation of risks to personal data V. Establish security measures applicable to personal data and identify those that are effectively implemented. VI. Analyze the gaps between existing security measures and those measures that are missing to protect personal data. VII. Prepare a work plan for the implementation of the missing security measures resulting from the gap analysis. VIII. Conduct reviews and audits. IX. Train personal data processors, and X. Keep records of personal data storage media.	HUAWEI CLOUD's information asset classification is monitored and managed by a dedicated tool to form an asset list, and each asset is assigned an owner. For personal data, HUAWEI CLOUD regularly combs through the list of personal data assets and identifies the corresponding asset owners through Privacy Impact Assessment (PIA). HUAWEI CLOUD attaches great importance to the security of users' data and information assets, and its security strategy and policy include a strong focus on data protection. HUAWEI CLOUD will continue to embrace industry-leading standards for data security lifecycle management and adopt best-of-breed security technologies, practices, and processes across a variety of aspects, including identity authentication, privilege management, access control, data isolation, transmission, storage, deletion, and physical destruction of storage media. In short, HUAWEI CLOUD will always strive toward the most practical and effective data protection possible in order to best safeguard the privacy, ownership, and control of our tenants' data against data breaches and impacts on their business. HUAWEI CLOUD has developed the Privacy Risk Assessment (PIA)

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
	HUAWEI CLOUD shall ensure that persons involved in any stage of personal data processing must maintain the confidentiality of such data and that this obligation shall continue even after their relationship with the data subject or with HUAWEI CLOUD has ended.	and Data Protection Risk Assessment (DPIA) to identify privacy and personal data protection risks from multiple dimensions. Each business unit regularly performs risk assessments on its own by identifying whether personal data is involved, sorting out data lists and information flows, identifying HUAWEI CLOUD's role in data processing, identifying DPIA and PIA requirements, and identifying compliance with checklists, and other steps as required. The risk assessment covers all aspects of privacy and personal data protection, including notification, choice and consent, personal data collection, use, retention and disposal, data subject access, third-party disclosure, cross-border transfer, and other aspects of compliance with applicable laws and regulations. The purpose of the risk assessment is to identify risks to privacy and personal data protection in HUAWEI CLOUD, assign a risk rating based on the likelihood and impact of the risk, formally document the assessment through a risk assessment report, and develop risk mitigation measures and plans. HUAWEI CLOUD has a dedicated audit team that regularly evaluates the compliance and effectiveness of strategies, procedures, supporting measures and indicators. In addition, independent third-party assessment agencies also provide independent assurance. These auditors assess the security, integrity, and confidentiality of information and resources by performing regular security assessments and compliance audits or inspections (such as SOC, ISO standards, PCIDSS audits), so as to conduct independent assessment of risk management content/process.

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
		HUAWEI CLOUD ensures that all employees' qualifications capabilities, and behavior comply with privacy protection requirements and requires employees to pass privacy protection appraisal every year. HUAWEI CLOUD has sorted out positions related to privacy protection and clearly defined the responsibilities of these positions. HUAWEI CLOUD also conducts background investigation and skill appraisal for new employees to ensure that they meet the requirements. Employees responsible for privacy protection are required to participate in skill training and pass appraisals. HUAWEI CLOUD has developed a media management standard that requires storage media to be kept in a controlled access area, and all storage media must be managed by including them in the media management process. The confidentiality agreement signed between HUAWEI CLOUD and the employee stipulates the confidentiality content and confidentiality period, and the confidentiality obligation remains even after the job is terminated.
Security measures document	HUAWEI CLOUD shall prepare a security measures document that lists the above security measures. HUAWEI CLOUD must update the security measures document when the following events occur: I. Modifications to the security measures or processes are made for their continuous improvement, arising from revisions of the security policy of HUAWEI CLOUD. II. Substantial modifications are made in the processing arising from a change in the level of risk.	HUAWEI CLOUD has established a Privacy Information Management System (PIMS) for organization-wide privacy management in accordance with ISO 27701 international standard requirements, implementing documented privacy policies and procedures to provide guidance for personal data processing. HUAWEI CLOUD reviews the information security and privacy information management system documentation at least once a year and updates it as needed to reflect changes in business objectives or risk

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
	III. A breach occurs during the processing of personal data. IV. Other circumstances that affect personal data have occurred. In the case of sensitive personal data, HUAWEI CLOUD shall review, and if necessary update the security document once a year.	environments.
Personal data retention period	When personal data is no longer necessary for the purposes set forth in the Privacy Notice provided to the data subject or in applicable law or the purposes for which the personal data was processed have been fulfilled, HUAWEI CLOUD shall cancel it and then block it for subsequent suppression. Personal data collected to fulfill a contractual obligation shall be removed after 72 months from the date the contractual obligation is no longer fulfilled. HUAWEI CLOUD must establish and document procedures for the retention, blocking and suppression of personal data, including the retention period. Personal data shall not be retained for longer than is necessary to achieve the purpose of the processing and shall comply with the laws applicable to the matter in question, taking into account the administrative, accounting, tax, legal and historical aspects of the information in question.	HUAWEI CLOUD regularly reviews the collection, use and disclosure purposes of personal data, and anonymizes or deletes personal data that are no longer needed. HUAWEI CLOUD has a personal data retention mechanism in place, and we will retain your personal data for as long as necessary to fulfill the purposes described in the Privacy Statement or to fulfill the purposes set forth in applicable law, unless the retention period needs to be extended as required by law or at your request. In the event that your personal data is retained beyond the retention period and we are not required by law to continue processing your specific personal data, we will delete or anonymize your personal data as required by applicable law. HUAWEI CLOUD keeps complete records of personal data processing activities, and each service lists the categories of data subjects, types of personal data, purposes of collecting personal data, flow of personal data, retention period and security measures taken in the assessment records by conducting privacy impact assessment.
Data processor or other third party	If personal data is processed by a data processor or other third party, HUAWEI CLOUD shall take the necessary measures to ensure that the data processor complies with the personal data protection principles established by this Law	HUAWEI CLOUD conducts due diligence and privacy and security capability assessment for all suppliers as required. The privacy protection obligations and requirements of applicable laws and regulations for a supplier as a

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
	and always complies with the Privacy Notice provided to the data subject. The relationship between HUAWEI CLOUD and the data processor must be established by contract or other legal instrument and allow its existence, scope and content to be proven. HUAWEI CLOUD shall bring to the attention of the data processor any request for correction, cancellation or withdrawal of consent of the data subject with respect to his or her personal data and ensure that the processor executes the corresponding request.	processor/sub-processor are specified in the contract to ensure that the supplier meets customers' privacy protection requirements. For other scenarios where HUAWEI CLOUD may disclose data to third parties in accordance with laws, see the **Privacy Statement**.
Corrective measures and notification of security breaches	Personal data security breaches that occur at each processing stage include loss or unauthorized destruction; theft, misplacement, or unauthorized copying; unauthorized use, access, or processing, and unauthorized corruption, alteration, or modification. In the event of a security breach of personal data, HUAWEI CLOUD must analyze why it occurred and implement corrective, preventive, and improvement measures to make the security measures adequate to avoid a recurrence of the breach. In the event of an information security breach, HUAWEI CLOUD must notify data subjects of security incidents that seriously damage the property or non-monetary rights of data subjects immediately after the incident has been confirmed and action has been taken to conduct an exhaustive review of the scale of the incident, so that the compromised data subject can take appropriate measures. The notification should include at least the following: the nature of the security incident, the personal data that has been compromised, recommendations to the data	HUAWEI CLOUD has set up a 24/7 professional security incident response team. This team discloses personal data breaches in a timely manner in compliance with applicable laws and regulations and executes the adequate contingency plan and recovery process to reduce the impact on customers. HUAWEI CLOUD formulates the classification and escalation principles of information security incidents, ranks them according to their degree of impact on the personal data subjects' business, initiates the notification process according to the notification mechanism of security incidents, and notifies personal data subjects of the incident. When serious events occur and have or may have a serious impact on multiple customers, HUAWEI CLOUD will promptly notify customers of events with an announcement. The contents of the notification shall at least include a description of the event, the cause, impact, measures taken by HUAWEI CLOUD and the measures recommended for customers. In addition, necessary

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
	subject on what measures they can take to protect their interests, immediate implementation of corrective measures, and ways for the data subject to obtain more information. HUAWEI CLOUD shall immediately report any security breach that has a significant impact on the property or moral rights of the data subject at any stage of personal data processing to the data subject so that the latter can take appropriate action to safeguard its rights.	regulatory filing will be conducted in accordance with local regulations.
Response to the rights of the data subject	HUAWEI CLOUD shall establish mechanisms to provide data subjects with remote or local electronic means of communication or other means it deems appropriate to ensure that data subjects can exercise their rights of access, correction, cancellation and objection (ARCO rights) at any time, and shall designate a personal data officer or department responsible for processing requests from data subjects to exercise their rights under this Law. HUAWEI CLOUD shall notify the data subject of its decision on whether to accept the ARCO rights request within 20 business days from the date of receipt. The decision shall be effective within 15 business days from the date of notification. If the request cannot be processed due to insufficient or inaccurate information provided by the data subject in its rights request, HUAWEI CLOUD shall request the data subject to provide additional information within 5 business days after receiving the request. If HUAWEI CLOUD does not hold the personal data of the requester, it shall also respond to the request within 20 business days of receipt.	HUAWEI CLOUD protects customers' rights to access and correct their personal data as data subjects. For customers to exercise their right to access and correct their personal data, HUAWEI CLOUD provides special channels to receive requests from customers and is equipped with a professional team to respond to customer requests related to personal data and privacy protection. In response to reasonable requests from customers, HUAWEI CLOUD's professional team completes processing and provides feedback to customers within the time specified in the legal regulations and internal specifications. When a personal data subject requests the deletion of his or her personal data, HUAWEI CLOUD will respond to the personal data subject's right to anonymize or delete his or her personal data for security purposes, in addition to complying with the requirements of applicable laws and regulations. When a customer cancels his or her HUAWEI CLOUD account, HUAWEI CLOUD will anonymize or delete the personal data that is no longer needed after the storage period ends, in addition to

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
	When a data subject requests confirmation that the processing of his or her personal data has ceased, HUAWEI CLOUD shall respond explicitly. Compliance with access rights may be by on-site access (HUAWEI CLOUD specifies an access period of no less than 15 business days), or by issuing copies or using magnetic, optical, audio, visual or holographic media, and other information technologies considered in the Privacy Notice, and HUAWEI CLOUD shall ensure readability of the format. HUAWEI CLOUD shall provide personal data free of charge after confirming the identity of the data subject and shall not use any service or means with fees as the only way to make a request to exercise ARCO rights. If the data subject makes a request to cancel his/her personal data, HUAWEI CLOUD shall respond within 20 business days of receiving the request, notify the data subject of the blocking period in the response, and begin blocking the data within 15 business days after the response accepts the data subject's right of cancellation. During the blocking period, HUAWEI CLOUD shall avoid processing other than storage and access, and take appropriate security measures for the data. The length of the blocking period shall be the limitation period of the lawsuit arising from the applicable legal relationship or the period specified in the contract, after which HUAWEI CLOUD shall formally cease any processing of personal data and suppress personal data. After the purpose of the processing has been achieved, HUAWEI CLOUD must cease processing the	complying with applicable laws and regulations.

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
	collected data after the blocking period and subsequently eliminate, purge, or destroy such data. If a data subject believes that HUAWEI CLOUD has violated the provisions of this Law in responding to the rights of the data subject, it has the right to submit a request to the supervisory authority to initiate a rights protection procedure. After the supervisory authority receives the request and sends it to HUAWEI CLOUD, HUAWEI CLOUD shall respond in writing with evidence within 15 business days. The supervisory authority will decide on the rights protection request after analyzing the evidence, and if the decision is in favor of the data subject, HUAWEI CLOUD shall be ordered to take necessary actions to respond to the protected data subject's rights within 10 business days after receiving the notification or within a longer period of time specified in the decision, and shall report in writing to the supervisory authority on the status of compliance with the decision within 10 business days.	
Domestic and international transfer of personal data	The consent of the data subject is required for any transfer of personal data, whether domestic or international, with the exceptions provided for in this law such as legal requirements, medical and health reasons, transfer to related companies, contractual necessity, protection of public interest, judicial reasons, etc. If HUAWEI CLOUD intends to transfer personal data to a domestic or foreign third party other than the data processor, it must provide that third party with a Privacy Notice and the purposes for which the data subject restricts the data processing. The data will be processed as agreed in the Privacy Notice, and	HUAWEI CLOUD has set up a team of privacy protection experts to assess the level of personal data protection provided by the countries involved in data transfer, and for the countries and regions where it does business, HUAWEI CLOUD also has dedicated legal and privacy protection staff to help HUAWEI CLOUD take the necessary measures in accordance with the requirements of applicable privacy regulations.

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Controller)	Measures Taken by HUAWEI CLOUD
	the third party recipient will have the same obligations as the HUAWEI CLOUD transferring the data. Both domestic and international transfers should be done through a formalized mechanism, such as contracts and other legal instruments that HUAWEI CLOUD can use when transferring personal data, which contain at least the same obligations as those to which HUAWEI CLOUD is subject, as well as conditions under which the data subject agrees to the processing of its personal data.	

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Processor)	Measures Taken by HUAWEI CLOUD
Obligations to process personal data	For processing performed on behalf of the data controller, HUAWEI CLOUD shall be obligated to: I. Process personal data only in accordance with the instructions of the data controller. II. Not process personal data for purposes other than those directed by the data controller. III. Implement the security measures required by law, these regulations, and other applicable laws and regulations. IV. To maintain the confidentiality of personal data to be processed. V. To erase personal data after the end of the legal relationship with the data controller or on the instructions of the data controller, provided that there is no legal requirement to keep such personal data. VI. Not to transfer personal data except on the basis of a decision of the data controller, subcontracting or if requested by a competent	HUAWEI CLOUD, as a data processor, only follows the customer's instructions for personal data processing operations, and the purpose and scope of content data collection is managed by the customer itself. HUAWEI CLOUD attaches great importance to the security of users' data and information assets, and its security strategy and policy include a strong focus on data protection. HUAWEI CLOUD will continue to embrace industry-leading standards for data security lifecycle management and adopt best-of-breed security technologies, practices, and processes across a variety of aspects, including identity authentication, privilege management, access control, data isolation, transmission, storage, deletion, and physical destruction of storage media. In short, HUAWEI CLOUD will always strive toward the most practical and effective data protection possible in order to best safeguard the privacy,

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Processor)	Measures Taken by HUAWEI CLOUD
	authority.	ownership, and control of our tenants' data against data breaches and impacts on their business. HUAWEI CLOUD provides computing, storage, database, network, or other services to customers, and customers have many options to encrypt their content data when using the services, and HUAWEI CLOUD is not allowed to access or use customer content data without customer consent. For customer content data, when the customer initiates data deletion operations or needs to delete data due to the expiration of the service, HUAWEI CLOUD will strictly follow applicable laws and regulations, as well as agreement with customers, delete the stored customer data in accordance with data destruction standards and ensure that the data is not recoverable. Customer can control the entire lifecycle of their content data on HUAWEI CLOUD and manage their content data according to their specific needs.

4.4 HUAWEI CLOUD's Compliance Measures in Response to the General Law for the Protection of Personal Data in Possession of Obligated Subjects

According to the requirements of the Obligated Subjects Data Protection Law, when customers fall under the scope of obligated subjects as defined in this Law and perform data processing, HUAWEI CLOUD, as a cloud service provider, assumes the role of a data processor and is regulated by the provisions of this Law for data processors. HUAWEI CLOUD actively responds and fulfills its obligations by adopting the following privacy protection mechanisms and technologies to comply with the requirements of Mexican privacy laws and regulations.

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Processor)	Measures Taken by HUAWEI CLOUD
Obligations to process personal data	HUAWEI CLOUD does not have any decision-making authority over the scope and content of personal data processing activities, and its actions shall be limited to the terms specified by the data controller.	HUAWEI CLOUD, as a data processor, only follows the customer's instructions for personal data processing operations, and the purpose and scope of content data collection is managed by the customer itself.
Protection of personal data	HUAWEI CLOUD shall undertake to protect personal data in accordance with the principles and obligations set forth in this Law and the applicable regulations, which is a prerequisite for the transfer of personal data outside the territory of the Data Controller.	HUAWEI CLOUD has adopted strict administrative and technical controls to ensure personal data security in the access, transfer, storage, processing and other stages of personal data lifecycle. • In terms of authentication, strict password policy and multi-factor authentication are adopted; • In the aspect of permission management, role-based access control and permission management for operation and maintenance personnel is implemented; • In terms of data storage and transmission, sensitive data encryption is adopted; • In terms of data processing, monitoring and auditing of access to critical systems through logging and auditing of data processing is adopted. Customers can also verify the privacy and security controls within HUAWEI CLOUD's environment through HUAWEI CLOUD security reports or certifications obtained. HUAWEI CLOUD has obtained multiple certifications from privacy compliance related international standard, including ISO 27701, ISO 29151, ISO 27018, BS 10012, SOC, privacy audit reports (please refer to Chapter 6 for a detailed introduction of certifications) Among all the international standards, ISO27018 is the international code of conduct focusing on the protection of

Core Requirements	Specific Requirements Applicable to HUAWEI CLOUD (As Data Processor)	Measures Taken by HUAWEI CLOUD
		personal data regarding cloud, its adoption indicates that HUAWEI CLOUD has a complete personal data protection management system.

5 How HUAWEI CLOUD Supports Customers to Comply with Mexican Privacy Protection Laws and Regulations

5.1 Customer's Privacy Protection Responsibilities under the Federal Law on the Protection of Personal Data held by Private Parties and its Regulations

When the customer is a private subject who decides to process personal data and uses HUAWEI CLOUD's services to provide services to others, the customer is a data controller as defined in the Private Data Protection Law and its regulations, and shall follow the compliance requirements of this Law and its regulations for data controllers. When the customer is a private subject entrusted by the data controller to process personal data, the customer is a data processor as defined in this Law and shall follow its compliance requirements for data processors. For the two different roles of customers, HUAWEI CLOUD, as a cloud service provider, will provide compliance support in the following areas to assist customers in achieving compliance through HUAWEI CLOUD's services. The following specific requirements applied by HUAWEI CLOUD incorporate the requirements of the Private Data Protection Law as well as supplementary instructions of its regulations.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
Measures to comply with the principles of personal data processing	The customer is subject to the principles of legality, consent, information, quality, purpose, fidelity, proportionality, and accountability as provided by law. To achieve this, the Customer may use standards, best international practices, corporate policies, self-regulatory arrangements, or any other mechanism deemed sufficient to achieve this purpose. Measures should include, at a	HUAWEI CLOUD provides customers with a variety of privacy protection technologies and services, including access control and identity authentication, data encryption, logging and auditing, to help customers protect their personal data according to their business needs. HUAWEI CLOUD has a dedicated team to support communication and contact with customers, and customers can seek assistance from

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	minimum: I. The development of privacy policies and programs that are binding and enforceable within the Customer's organization II. The implementation of training programs designed to develop, update and raise awareness among personnel of their obligations to protect personal data III. Establish internal oversight and monitoring systems and conduct external inspections or audits to verify compliance with the privacy policy IV. Provide dedicated resources for the implementation of privacy programs and policies V. Implement a process to address risks to personal data protection resulting from the implementation of new products, services, technologies, and business models, and to mitigate those risks VI. Periodically review security policies and programs to identify needed changes. VII. Establish procedures for receiving and responding to data subject questions and complaints VIII. Establish mechanisms for compliance with the privacy policy and program and sanctions for violations of the policy and program IX. Establish measures for the protection of personal data, i.e., a set of technical and administrative actions that will enable customers to ensure compliance with the principles and obligations set forth in laws and regulations. X. Establish measures for the tracking of personal data, i.e. actions, measures and technical procedures that allow for the tracking of personal data when it is processed.	HUAWEI CLOUD through the service ticket page.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
Privacy Notice	The Customer shall inform the data subject, through a Privacy Notice, prior to the collection of personal data, of the personal data collected from it and the purposes for which it is processed, in particular with regard to processing for marketing, advertising or commercial exploration and processing for decision-making without human intervention. The Privacy Notice should also include the name and address of the customer's company, any transfers of personal data, and the use of remote or local electronic, optical or other technical means of communication mechanisms when the customer automatically obtains personal data, and the manner in which the data subject objects to their use. Mechanisms that allow the data subject to object to what is stated in the Privacy Notice, restrictions on the use or disclosure of data and withdrawal of consent, the manner in which the rights of the data subject are exercised, the method of notifying the data subject of changes to the Privacy Notice, and the processing of sensitive personal data shall also be communicated through the Privacy Notice. The Privacy Notice may be provided to the data subject orally, on paper, electronically, in video or audio format, or through any other technology. The Privacy Notice must be simple and contain the necessary information in language, structure and design that is clear and easy to understand. If personal data is not obtained directly from the data subject, the customer must notify the data subject of any changes to the Privacy Notice. In the event that it is not possible to provide the Privacy Notice to the data subject, or in the event of disproportionate	Some of the products and services provided by HUAWEI CLOUD provide customers with an interface to embed Privacy Statements and a function to record relevant operations. Customers can inform the data subject of the type of personal data to be collected, the purpose of use, the retention period, and other information in the Privacy Statement. Customers are advised to evaluate their products and services, and if the conditions for notification are met, they are advised to implement the notification in accordance with legal requirements.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	payment due to the excessive number of data subjects or the age of the data, the customer may request the supervisory authority (INAI, the National Institute for Transparency, Access to Information and Personal Data Protection) to implement compensatory measures using mass communication media, if authorized.	
Processing sensitive personal data	The Customer may collect sensitive personal data: when required by law; in cases involving national security, public order, health and safety and the protection of the rights of third parties; when required for a legitimate, specific purpose based on an explicit activity or purpose. Customers are required to obtain express consent for the processing of sensitive personal data, financial or asset-related personal data communicated through the signature of the data subject, an electronic signature or any authentication mechanism established for this purpose.	The **Data Security Center service (DSC)** provided by HUAWEI CLOUD to customers can help customers perform basic data security operations such as data classification and classification, data security risk identification, data watermark traceability, and data desensitization. It can accurately and efficiently identify sensitive data and precisely identify sensitive data in the database according to sensitive data discovery policies, and realize full-stack sensitive data protection based on a variety of pre-set desensitization algorithms and user-defined desensitization algorithms.
Consent of the data subject	All processing of personal data shall be subject to the consent of the data subject. Implied consent is generally valid unless the data subject is required by law to give explicit consent. If the data subject does not object to the Privacy Notice, his or her implied consent to the processing of the data may be deemed to be given, provided that the Privacy Notice contains sufficient information. If the customer intends to process the data for purposes incompatible or similar to those stated in the Privacy Notice, the consent of the data subject must be obtained again. The data subject may refuse or withdraw his consent to the	The functions provided in some of the cloud products and services provided by Huawei or the capabilities built by itself better practice the requirements of privacy protection regulations clearly informing data subjects. For example, customers can embed the customer's privacy policy through the interface provided by HUAWEI CLOUD, suggesting that the customer clearly state the purpose of personal data processing and the legal basis for satisfaction in the privacy policy, and HUAWEI CLOUD can provide the customer with the ability to record the operation record of the data subject's consent.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	processing of the data at any time and may also object to the processing of his data for unnecessary purposes. However, refusal, withdrawal of consent or objection to processing by the data subject does not terminate the processing based on the necessary purposes and the processing based on the legal relationship between the customer and the data subject.	
Measures taken to protect the security of personal data	In order to establish and maintain the security of personal data, the customer must take the following actions into account: I. Prepare an inventory of personal data and processing systems. II. Define the responsibilities and duties of the persons processing personal data. III. Conduct a risk analysis of personal data, including the identification of hazards and estimation of risks to personal data IV. Establish security measures applicable to personal data and identify those measures that are effectively implemented. V. Analyze the gaps between existing security measures and those measures that are missing to protect personal data. VI. Prepare a work plan for the implementation of the missing security measures resulting from the gap analysis. VII. Conduct reviews and audits. VIII. Train personal data processors, and IX. Maintain records of personal data storage media. The Customer shall ensure that persons involved in any phase of personal data processing must maintain the confidentiality of such data, and that this obligation will continue even after the end of the	HUAWEI CLOUD provides customers with a variety of privacy protection technologies and services, including **Identity and Access Management (IAM)**, **Data Encryption Workshop (DEW)**, **Log Tank Service (LTS)**, and **Cloud Trace Service (CTS)**, providing customers with access control and authentication, data encryption, logging, and auditing functions. It helps customers to protect their personal data according to their business needs.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	relationship between the Customer or the Data Subject and the Data Subject.	
Personal data retention period	When personal data is no longer necessary for the purposes set forth in the Privacy Notice provided to the data subject or in applicable law or when the purposes for which the personal data was processed have been fulfilled, the customer shall cancel it and then block it for subsequent suppression. Personal data collected for the fulfilment of contractual obligations shall be removed after 72 months from the date on which the contractual obligations are no longer fulfilled. The customer must establish and document procedures for the retention, blocking and suppression of personal data, including the retention period. Personal data shall not be kept for longer than is necessary to achieve the purposes of processing and shall comply with the laws applicable to the matter in question, taking into account the administrative, accounting, tax, legal and historical aspects of the information in question.	The data deletion function is provided in most of HUAWEI CLOUD's products or services, and for customer content data, customers can actively perform data deletion operations.
Data processor or other third party	If personal data is processed by a data processor or other third party, the customer shall take the necessary measures to ensure that the data processor complies with the principles of personal data protection established by this law and always complies with the Privacy Notice provided to the data subject. The relationship between the customer and the data processor must be established by contract or other legal instrument and allow its existence, scope and content to be proven. The customer shall bring to the	The customer can inform its users of the policy on personal data handling by embedding the function of agreeing to or revoking the Privacy Statement and recording the related operation records through the interface of signing and querying the Privacy Statement provided in some HUAWEI CLOUD products and services.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	attention of the data processor any request for correction, cancellation or withdrawal of consent of the data subject with respect to his personal data and ensure that the processor executes the corresponding request.	
Personal data processing in cloud computing	For the processing of personal data in services, applications and infrastructure in the cloud, where the customer complies with the same requirements through general contractual terms or conditions, such services may only be used if the cloud provider meets the following requirements: At a minimum, the following requirements are complied with: I. Have and apply a personal data protection policy that is consistent with the applicable principles and obligations set forth in this law and regulations. II. Be transparent about the subcontracting of information about the services provided. III. Not to attach to the provision of the services conditions for obtaining subjectship of the data covered by the services IV. Confidentiality of the personal data for which it provides services. Have at least the following mechanisms: I. Publish changes to its privacy policy or the conditions under which it provides its services. II. Allow customers to limit the type of processing of personal data for which they provide services. III. Establish and maintain appropriate security measures to protect the personal data for which it provides services. IV. Ensure that personal data is suppressed and that the controller is able to recover such personal data once the services provided to the	In order to protect customers' personal data and help customers build privacy protection for their business on the cloud, HUAWEI CLOUD has established and continuously improved the HUAWEI CLOUD Business Privacy Protection Management System. Guided by the vision of "to respect and protect customer privacy, and to be a cloud partner that provides trustworthy, easy-to-use services", HUAWEI CLOUD refers to the widely recognized privacy protection principles in the industry and adopts the concept of privacy integration into design PbD to integrate privacy protection into every business activity, forming a unique privacy protection management system for HUAWEI CLOUD. In order to cooperate with customers exercising supervision of service providers, HUAWEI CLOUD Online's HUAWEI CLOUD **Customer Agreement** divides the security responsibilities of customers and HUAWEI CLOUD, and the HUAWEI CLOUD **Service Level Agreement** specifies the level of service provided by HUAWEI CLOUD. At the same time, HUAWEI CLOUD has also developed an offline contract template, which can be based on the specific requirements of the customer, in which HUAWEI CLOUD is required to notify the customer if it hires a subcontractor and is responsible for the subcontracted services. HUAWEI CLOUD deeply

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	customers are terminated. V. Block access to personal data by persons without proper authority and inform the Customer if access is officially requested by the competent authorities. The Customer shall ensure in all cases the use of services that ensure proper protection of personal data.	understands the importance of the customer's content data to the customer's business, and HUAWEI CLOUD adheres to a neutral attitude to ensure that the customer's data is owned by the customer, used by the customer, and creates value for the customer. Customers have full control over their content data when using HUAWEI CLOUD. The confidentiality agreement signed between HUAWEI CLOUD and its employees stipulates the confidentiality content and confidentiality period, and the confidentiality obligation remains even after the employee's position is terminated. HUAWEI CLOUD provides the **Privacy Statement** on its website and regains user consent when it changes. HUAWEI CLOUD provides different types of services and products for customers to choose at their own discretion, providing personal data processing functions including storage and analysis. The data deletion function is provided in most of HUAWEI CLOUD's products or services, and for customer content data, customers can take the initiative to perform data deletion operations. Customers can manage user accounts that use cloud resources through HUAWEI CLOUD's **Identity and Access Management (IAM)**. Each HUAWEI CLOUD customer has a uniquely identifiable user ID in HUAWEI CLOUD. In addition, HUAWEI CLOUD provides a variety of user authentication mechanisms, including account passwords and multi-factor authentication.
Corrective measures and	Personal data security breaches that occur at each stage of processing	Customers are advised to consider how to manage and protect personal

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
notification of security breaches	include loss or unauthorized destruction; theft, misplacement or unauthorized copying; unauthorized use, access or processing, and unauthorized damage, alteration or modification. In the event of a security breach of personal data, the customer must analyze the reasons for its occurrence and implement corrective, preventive and improvement measures so that security measures are adequate to avoid a recurrence of the breach. In the event of an information security breach, the Customer must notify the data subject of those security incidents that seriously damage the property or non-monetary rights of the data subject immediately after the incident has been confirmed and action has been taken to conduct an exhaustive review of the scale of the incident so that the damaged data subject can take appropriate measures. The notification shall contain, at a minimum, the following: the nature of the security incident, the personal data that was compromised, recommendations to the data subject as to what measures he or she can take to protect his or her interests, the immediate implementation of corrective measures, and the means by which the data subject can obtain additional information. In the event of a security breach that has a significant impact on the property or moral rights of the data subject at any stage of the processing of personal data, the customer shall immediately report it to the data subject so that the latter can take appropriate action to defend its rights.	data security to prevent the occurrence of personal data leakage, and in case of leakage, they should notify data subjects and regulators in a timely manner according to the corresponding laws and regulations. HUAWEI CLOUD has a dedicated team to ensure communication and contact with customers. When a data leakage event occurs on the customer side, HUAWEI CLOUD will cooperate with customers in the personal data leakage investigation and response process. HUAWEI CLOUD provides **Log Tank Service (LTS)** and **Cloud Trace Service (CTS)** for the discovery of security breaches, and also assists customers in the forensics, investigation, analysis and disposal process of security breaches.
Response to the rights of the data	The Customer shall establish mechanisms to provide the Data Subject with remote or local electronic means of communication	HUAWEI CLOUD has a dedicated team responsible for communication with customers, and customers can seek assistance

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
subject	or other means it deems appropriate to ensure that the Data Subject may exercise the rights of access, correction, cancellation and opposition (ARCO Rights) at any time, and shall designate the personal data officer or department responsible for processing requests from the Data Subject to exercise the rights referred to in this Law. The Customer shall notify the data subject of its decision on the admissibility of the request for ARCO rights within 20 working days from the date of receipt of the request. The decision shall take effect within 15 working days from the date of the notification. If the request cannot be processed due to insufficient or inaccurate information provided by the Data Subject in its request for rights, the Customer shall request additional information from the Data Subject within 5 business days of receipt of the request. If the Customer does not hold personal data of the requestor, it shall also respond to the request within 20 business days of receipt. When the data subject requests confirmation that the processing of his personal data has ceased, the customer shall respond explicitly. Compliance with the right of access may be by means of on-site access (the period of access specified by the Customer shall not be less than 15 working days) or by issuing copies or using magnetic, optical, acoustic, visual or holographic media, as well as other information technologies considered in the Privacy Notice, and the Customer shall ensure the readability of the format. The Customer shall provide the personal data free of charge upon confirmation of the identity of the	from HUAWEI CLOUD through the service ticket page.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	data subject and shall not use any service or means with a fee as the only way to make a request to exercise ARCO's rights. If the Data Subject requests the cancellation of his personal data, the Customer shall respond within 20 business days of receiving the request, inform the Data Subject of the blocking period in the response, and begin the blocking of the data within 15 business days of the response accepting the Data Subject's right of cancellation. During the blocking period, Customer shall refrain from processing other than storage and access, and shall take appropriate security measures for the data. The length of the blocking period shall be the limitation period of the proceedings arising from the applicable legal relationship or the period stipulated in the contract, after which the Customer shall formally cease any processing of personal data and suppress personal data. After the purpose of the processing has been achieved, the Customer must cease processing the collected data after the blocking period and subsequently erase, purge or destroy such data. If the data subject considers that the customer has violated the provisions of this Law in response to the rights of the data subject, it has the right to submit a request to the supervisory authority to initiate a rights protection procedure. After the Supervisory Authority receives the request and sends it to the Customer, the Customer shall respond in writing, providing evidence, within 15 business days. The Supervisory Authority will decide on the request for protection of rights after analyzing the evidence, and if the decision is in	

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	favor of the data subject, the Customer will be ordered to take the necessary actions to respond to the protected data subject's rights within 10 business days after receiving the notification or within a longer period specified in the decision, and shall report in writing to the Supervisory Authority on the compliance with the decision within 10 business days.	
Domestic and international transfer of personal data	The consent of the data subject is required for any transfer of personal data, whether domestic or international, subject to the exceptions provided for in this Act such as legal requirements, medical and health reasons, transfer to the company concerned, contractual necessity, defense of the public interest, judicial reasons, etc. If the customer intends to transfer personal data to a third party, domestic or foreign, other than the data processor, he or she must provide that third party with a Privacy Notice and the purposes for which the data subject has restricted the data processing. The data processing will be carried out as agreed in the Privacy Notice and the third-party recipient will have the same obligations as the customer to whom the data is transferred. Both domestic and international transfers shall be made through a formalized mechanism, such as contracts and other legal instruments available to the customer for the transfer of personal data, which contain at least the same obligations as those imposed on the customer, as well as the conditions under which the data subject agrees to the processing of his or her personal data.	Customers are advised to assess the level of personal data protection provided by the countries involved in the data transfer and to formalize mechanisms for the cross-border transfer of personal data.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
Obligations to process personal data	For processing on behalf of the data controller, the customer shall be obliged: I. To process personal data only in accordance with the instructions of the data controller II. Not to process personal data for purposes other than those instructed by the data controller III. To implement the security measures required by law, these Regulations and other applicable laws and regulations IV. To maintain the confidentiality of personal data to be processed. V. Erase personal data after the end of the legal relationship with the data controller or on the instructions of the data controller, provided that there is no legal requirement to keep such personal data. Not to transfer personal data except on the basis of a decision of the data controller, subcontracting or if requested by the competent authorities.	Customers are advised to process personal data only in accordance with the instructions of the data controller and for the purposes specified by the data controller. HUAWEI CLOUD provides computing, storage, database, network, or other services to customers. Customers have many options to encrypt their content data when using the services, and HUAWEI CLOUD shall not access or use customer content data without customer's consent. The data deletion function is provided in most of HUAWEI CLOUD's products or services, and for customer content data, customers can proactively perform data deletion operations.
Use of subcontracting services	Any subcontracting of services by the Customer implies the processing of personal data, which must be authorized by the data controller and shall be carried out in the name and on behalf of the latter. After obtaining authorization, the Customer must formalize its relationship with the subcontractor by means of a contract or other instrument that allows proof of its existence, scope and content. The person or body corporate to which the subcontract is made will be subject to the same obligations imposed on the Customer by law, by these Regulations and by other applicable laws and regulations. The customer is obliged to prove	Customers are advised to obtain authorized consent from the controller before using subcontracting services and to sign a formal contract with the subcontractor.

	that the subcontracting was carried out under the authority of the Data Controller. When the contract or legal instrument formalizing the relationship between the Data Controller and the Customer contemplates that the latter may subcontract services, the Controller's authorization to the Customer will be understood as given through the terms in these documents. If the contract or legal instrument formalizing the relationship between the Data Controller and the Customer does not contemplate subcontracting, the Customer must obtain the authorization of the Data Controller prior to subcontracting.	

5.2 Customer's Privacy Protection Responsibilities under the General Law for the Protection of Personal Data in Possession of Obligated Subjects

When the customer is an obligated subject regulated by the Obligated Subjects Data Protection Law and decides on the processing of personal data, i.e. any authority, entity, organ and body of the Executive, Legislative and Judicial Powers, autonomous bodies, political parties, trusts and public funds, it is a data controller and shall meet the compliance requirements of this Law with respect to data controllers. When the customer is an obligated subject entrusted by the data controller to process personal data and use HUAWEI CLOUD's services, the customer is a data processor as defined in the Law and shall meet its compliance requirements for data processors. For the two different roles of customers, HUAWEI CLOUD will provide compliance support to customers in the following areas.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
Measures to comply with the principles of personal data processing	The Customer shall comply with the principles of lawfulness, purpose, fidelity, consent, quality, proportionality, information and responsibility in the processing of personal data and with the rights or obligations conferred by applicable regulations. Also all processing of personal data carried out by the customer must have a specific,	HUAWEI CLOUD provides customers with a variety of privacy protection technologies and services, including access control and authentication, data encryption, logging, and auditing, to help customers protect their personal data according to their business needs. HUAWEI CLOUD has a dedicated

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	legal, clear and legitimate purpose and be adequate, relevant and strictly necessary for the purpose of the processing. The Customer may only process personal data for purposes other than those specified in the Privacy Notice if the Customer has the powers conferred by law or the consent of the data subject or if the data subject is the person who reported the disappearance. Among the mechanisms adopted by the Customer to comply with the principles of responsibility set forth in this Law shall be, at a minimum, the following: I. The allocation of resources authorized for this purpose for the implementation of personal data protection programs and policies II. The development of personal data protection policies and programs that are mandatory and enforceable within the Customer's organization III. Implement training and update programs to inform employees of their obligations and other responsibilities regarding personal data protection IV. Periodically review the personal data security policy and program to identify changes that may be required V. Establish a system of internal and/or external oversight and monitoring, including audits, to verify compliance with the personal data protection policy VI. Establish procedures for receiving and responding to inquiries and complaints from data subjects VII. Design, develop and implement its public policies, programs, services, computer systems or platforms, electronic applications or any other	team to support communication with customers, and customers can seek assistance from HUAWEI CLOUD through service ticket page.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	technology involving the processing of personal data, in accordance with the provisions set forth in this Law and other applicable provisions on the matter; and VIII. Ensure that its public policies, programs, services, computer systems or platforms, electronic applications or any other technology involving the processing of personal data comply, by default, with the obligations set forth in this Law and any other applicable provisions on the matter.	
Privacy Notice	The customer must inform the data subject, through the Privacy Notice, of the existence and main characteristics of the processing to which his personal data will be subjected, so that he can make an informed decision in this regard. In general, the Privacy Notice should be disseminated through electronic and physical means available to the customer. In order for a Privacy Notice to effectively perform its informative function, it must be drafted and organized in a clear and simple manner. When it is not possible to directly inform data subjects who are required to provide a Privacy Notice, or when this requires a disproportionate effort, the customer may implement compensatory measures for mass communication in accordance with the standards issued by the National Transparency, Access to Information and Personal Data Protection System for this purpose. The Privacy Notice shall be provided to the data subject in two ways: simplified and detailed. The simplified Privacy Notice shall contain the following information:	Some of the products and services provided by HUAWEI CLOUD provide customers with an interface to embed the Privacy Statement and the function to record relevant operations. Customers can inform the data subject of the type of personal data to be collected, the purpose of use, the retention period, and other information in the Privacy Statement. Customers are advised to evaluate their products and services and, if the conditions for notification are met, they are advised to implement the notification in accordance with legal requirements.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	I. The name of the customer. II. The purpose of the processing for which the personal data is obtained, distinguishing those purposes that require the consent of the data subject. III. When transferring personal data requiring consent, the following persons and contents must be informed: (a) The competent authorities, authorities, entities, institutions and government agencies of the three levels of government, as well as the natural or legal persons receiving the personal data; and (b) the purpose of the transfer. IV. The mechanisms and means available so that the data subject may, in appropriate cases, object to the processing and transmission of his or her personal data for purposes that require his or her consent, and V. A website where a detailed Privacy Notice can be accessed. The detailed Privacy Notice shall contain the following information: I. The address of the customer. II. The personal data that will be processed and identifying the sensitive personal data contained therein III. The legal basis for authorizing the processing to be carried out by the Customer. IV. The purposes for which the personal data will be accessed for processing, distinguishing those purposes for which the consent of the data subject is required. V. The mechanisms means and procedures that may be used to exercise ARCO's rights. VI. The address of the transparency department, and VII. The manner in which the	

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	customer will communicate changes to the Privacy Notice to the data subject.	
Processing sensitive personal data	The provisions of this law regarding the processing of sensitive personal data by data controllers are identical to those of the Private Data Protection Law	See section 5.1 "Processing sensitive personal data"
Consent of the data subject	The provisions of this law regarding the processing of sensitive personal data by data controllers are identical to those of the Private Data Protection Law	See section 5.1 "Consent of the data subject".
Measures taken to protect the security of personal data	In order to establish and maintain security measures for the protection of personal data, the Customer shall carry out at least the following interrelated activities: I. Establish an internal policy for the management and processing of personal data that takes into account the context in which the processing occurs and the life cycle of personal data, i.e., its collection, use and subsequent suppression II. Define the functions and obligations of the persons involved in the processing of personal data. III. To compile an inventory of personal data and processing systems IV. Conduct a risk analysis of personal data, taking into account the existing threats and vulnerabilities of personal data and the resources involved in processing them, such as, but not limited to, hardware, software, personnel of the Customer, etc. V. Analyze the gaps between existing security measures and those that are lacking in the Customer's organization. VI. Develop work plans for the implementation of missing security measures and measures for day-to-day compliance with	HUAWEI CLOUD provides customers with a variety of privacy protection technologies and services, including **Identity and Access Management (IAM)**, **Data Encryption Workshop (DEW)**, **Log Tank Service (LTS)**, and **Cloud Trace Service (CTS)**, providing customers with access control and authentication, data encryption, logging, and auditing functions. It helps customers to protect their personal data according to their business needs.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	policies for the management and processing of personal data. VII. Monitor and periodically review the implemented security measures, as well as the threats and breaches to personal data, and VIII. Design and implement different levels of training based on the roles and responsibilities of personnel in the processing of personal data. The Customer must establish controls or mechanisms whose purpose is to ensure the confidentiality of personal data by all persons involved in any phase of the processing of such data, an obligation that shall continue even after the end of their relationship with the controller.	
Databases held by security, prosecution and judicial agencies	According to the provisions of this Law, the collection and processing of personal data by the competent authorities of security, law enforcement and justice administration agencies is limited to those cases and categories of data that are necessary and proportionate for the exercise of functions related to national security, public safety, or for the prevention or prosecution of crimes. They must be stored in a database specifically created for this purpose. A high level of security measures should be established in this database to guarantee the integrity, availability and confidentiality of the data in order to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing. The processing of personal data by competent supervisory entities of security, law enforcement and judicial administration agencies, as well as the use of data stored in the database, must comply with the	Access control, network isolation, and other security configurations are provided in HUAWEI CLOUD products. HUAWEI CLOUD provides specialized security products to help customers improve a certain aspect of security, such as **Database Security Service (DBSS)**, **Advanced Anti-DDoS (AAD)**, and **Vulnerability Scan Service (VSS)**. HUAWEI CLOUD has been certified by several privacy compliance-related international standards to prove that HUAWEI CLOUD has sufficient safeguards in terms of technical capabilities and organizational capacity for data processing.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	data processing principles set forth in this Law. Private communications are inviolable. The interception of any private communication may be authorized only by the federal judicial authorities, at the request of the federal authority authorized by law or the head of the prosecutor's office of the corresponding federal entity.	
Personal data retention period	Personal data shall be blocked and suppressed at the end of the blocking period if the personal data is no longer needed to achieve the purposes described in the Privacy Notice. The Customer must establish and document procedures for the retention, blocking and suppression of personal data, which shall include its retention period. The relevant procedures must include mechanisms that allow the Customer to comply with the deadlines set for the suppression of personal data and to conduct periodic reviews of the need to retain personal data. Personal data shall not be kept for longer than is necessary to achieve the purposes for which it is processed and shall comply with the provisions applicable to the matter in question, taking into account the administrative, accounting, tax, legal and historical aspects of personal data.	The data deletion function is provided in most of HUAWEI CLOUD's products or services, and for customer content data, customers can actively perform data deletion operations.
Data processor or other third party	The relationship between the Customer and the Data Processor shall be formalized by a contract or any other legal instrument determined by the Customer in accordance with the applicable regulations and allowing for the certification of its existence, scope and content. The contract or legal instrument determined by the Customer must include at least the following general terms in relation to the services provided by the Data	The customer can inform its users of the policy on personal data handling by embedding the function of agreeing to or revoking the Privacy Statement and recording the related operation records through the interface of signing and querying the Privacy Statement provided in some HUAWEI CLOUD products and services.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	Processor: I. The processing of personal data in accordance with the instructions of the Customer. II. Avoiding the processing of personal data for purposes other than those instructed by the Customer III. To implement security measures in accordance with the applicable legal instruments IV. To notify the Customer in the event of a security breach of the personal data it processes in accordance with its instructions V. Maintain the confidentiality of the personal data processed. VI. Delete or return the personal data being processed once the legal relationship with the Customer has been fulfilled, as long as there are no legal provisions requiring the retention of personal data; and VII. Avoid transferring personal data unless the Customer decides to do so, or the transfer is due to subcontracting, or is expressly authorized by a competent authority. Agreements between the Customer and the Processor relating to the processing of personal data shall not violate the provisions of this Law and other applicable regulations, as well as the provisions of the corresponding Privacy Notice.	
Personal data processing in cloud computing	The provisions of this law that address the use of cloud computing by data controllers for personal data processing are the same as those of the Federal Act on the Protection of Privately Held Personal Data.	See section 5.1 "Personal data processing in the cloud computing".
Corrective measures and notification of security	Security breaches of personal data that occur at any stage of data processing include unauthorized loss or destruction; theft,	Customers are advised to consider how to manage and protect personal data security to prevent the occurrence of personal data

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
breaches	misplacement or unauthorized copying; unauthorized use, access or processing; and unauthorized damage, alteration or modification. In the event of a security breach, Customer shall analyze the cause of the breach and implement preventive and corrective measures in its work plan to adjust security measures and the processing of personal data to prevent a recurrence of the security breach. The Customer shall document the security breach, stating the circumstances of the breach, the date of occurrence, the cause, and the immediate and final corrective measures implemented. Customers must notify data subjects of breaches that seriously affect economic or moral rights and, as appropriate, the supervisory authority and the sponsoring agency of the federal entity, immediately after confirming that a breach has occurred and that action has been initiated to initiate an exhaustive review of the severity of the breach, so that affected data subjects can take appropriate measures to assert their rights. The notification shall contain, at a minimum, the nature of the incident, the personal data affected, a recommendation to the data subject on the measures that he or she may take to protect his or her interests, immediate corrective action and the means by which additional information may be obtained in this regard.	leakage, and in case of leakage, they should notify data subjects and regulators in a timely manner according to the corresponding laws and regulations. HUAWEI CLOUD has a dedicated team to ensure communication and contact with customers. When a data leakage event occurs on the customer side, HUAWEI CLOUD will cooperate with customers in the personal data leakage investigation and response process. HUAWEI CLOUD provides **Log Tank Service (LTS)** and **Cloud Trace Service (CTS)** for the discovery of security breaches, and also assists customers in the forensics, investigation, analysis and disposal process of security breaches.
Response to the rights of the data subject	The data subject or his representative may at any time request access, rectification, cancellation or opposition to the processing of his personal data. In order to exercise ARCO's rights, it is necessary for the customer to confirm the identity and personality of the data subject or his	HUAWEI CLOUD has a dedicated team responsible for communication with customers, and customers can seek assistance from HUAWEI CLOUD through the service ticket page.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	representative. It is possible to exercise the rights of ARCO by a person other than the data subject or his representative, as provided by law, by court order or in appropriate exceptional cases. According to the Civil Code, in the case of the exercise of ARCO rights by minors or persons in a state of confinement or incapacity, the rules of representation provided for in the same legislation shall apply. In the case of personal data concerning a deceased person, the right granted by this law may be exercised by the person who proves to have a legitimate interest, in accordance with the applicable legislation, provided that the right holder has duly expressed his or her will, or that there is a court order indicating this. The exercise of ARCO rights shall be free of charge. Under the applicable regulations, fees may only be charged to recover the costs of reproduction, authentication or provision. In the case of access to personal data, the law determining the cost of reproduction and authentication shall be determined taking into account that the amount allows or facilitates the exercise of the right. When the data subject provides the magnetic or electronic means or mechanism required to reproduce personal data, it shall be provided free of charge to the data subject. When the information involves the delivery of no more than 20 simple pages, it shall be provided free of charge. The Transparency Sector may waive the cost of reproduction and provision, depending on the socio-economic situation of the data subject. The Customer shall not establish any service or means for submitting a request for the exercise of ARCO rights that implies a fee for the data	

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	subject. The Customer shall establish simple procedures to enable the exercise of ARCO rights, whose response time shall not exceed 20 working days from the day following the receipt of the request. The response period may be extended once for justifiable reasons, up to a maximum of 10 business days, and the data subject must be notified within the response period. If the exercise of ARCO rights is acceptable, the Customer must make them effective within a period not exceeding 15 business days from the day following the date of receipt of the response notice by the Data Subject. For the request to exercise the ARCO rights, the Customer may not request more than: I. The name of the data subject and his residence or any other means of receiving the notification II. Documents proving the identity of the data subject and, where appropriate, the personality and identity of the representative III. If possible, the area responsible for processing the personal data and submitting the request to them IV. A clear and precise description of the personal data for which the request is intended to exercise any of the rights of the ARCO, except in the case of access rights V. A description of the ARCO rights to be exercised, or the content requested by the data subject, and VI. Any other element or document that will help locate the personal data. In the case of requests for access to personal data, the customer must comply with the request in the form	

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	requested by the data subject, unless there is a physical or legal impossibility that restricts it from copying personal data in this form, in which case the personal data must be provided in another form and justify and explain the reasons for such action. If the data protection request does not meet any of the requirements described in this article, and the supervisory authority or the guarantee agency does not have the elements to remedy the situation, the data subject will be notified once within 5 business days of the request to exercise the ARCO rights, allowing him or her to add the missing information within 10 business days from the day following the date of notification. When the Customer does not have the capacity to process a request to exercise ARCO rights, it shall inform the Data Subject of this situation within 3 business days of the request being made and, if it can be determined, it shall direct the Data Subject to a competent data controller to make the request. If the customer declares that no personal data exists in its files, records, systems or documents, such declaration shall be recorded in a resolution of the Transparency Board confirming the non-existence of personal data. If the customer notes that the request to exercise the ARCO rights differs from the rights provided for in this Law, it must re-establish the path by notifying the data subject. If the provisions applicable to the processing of certain personal data provide for a specific process or procedure for requesting the exercise of ARCO rights, the customer shall notify the data subject of the existence of ARCO rights within 5 business days of the	

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	request to exercise them, so that the latter may decide whether to exercise its rights through the specific process or through the procedure institutionalized by the customer for the processing of requests to exercise ARCO rights in accordance with the provisions of this Law Exercise of its rights.	
Personal Data Protection Impact Assessment	Intensive or related processing of personal data shall be deemed to have taken place when there is an inherent risk to the personal data to be processed, when processing sensitive personal data and when the transfer of personal data has taken place or is intended to take place. When the Customer intends to implement or modify public policies, computer systems or platforms, electronic applications or any other technology that it considers to imply intensive or relevant processing of personal data, the Customer must carry out an impact assessment of personal data protection and submit it, as appropriate, to the supervisory authority or the guarantee body, which may issue non-binding recommendations dedicated to the protection of personal data. The content of the personal data protection impact assessment shall be determined by the national transparency, access to information and personal data protection system. The Customer conducting the personal data protection impact assessment shall submit it to the supervisory authority or the guarantee body 30 working days before the date on which it intends to implement or modify public policies, computer systems or platforms, electronic applications or any other technology, in order to facilitate the latter's issuance of the corresponding non-binding	Customers are advised to conduct a personal data protection impact assessment based on an assessment of whether personal data is involved in intensive or relevant processing and, if so, in accordance with the National System of Transparency, Access to Information and Protection of Personal Data, and to submit the impact assessment to the supervisory authority or guarantee body within the specified deadline.

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers
	recommendations. A personal data protection impact assessment is not required when the Customer believes that its intended effects may be jeopardized by the possible implementation or modification of public policies, computer systems or platforms, electronic applications or any other technology involving intensive or related processing of personal data, or in case of emergency or urgency.	
Domestic and international transfer of personal data	Any domestic or international transfer of personal data shall be subject to the consent of the data subject, with the exceptions provided for by law, court order, reasonable authorization by the competent authorities, etc., as provided for in this Law. The Customer may transfer or forward personal data outside the national territory only if the receiving third party or data processor undertakes to protect the personal data in accordance with the principles and obligations set forth in this Law and the applicable regulations. In any transfer of personal data, the Customer shall communicate to the recipient of the personal data a Privacy Notice, in accordance with which the personal data is processed. All transfers must be formalized through the execution of contractual provisions, cooperation agreements or any other legal instruments in accordance with the provisions applicable to the Customer, in order to demonstrate the scope of processing of personal data, as well as the obligations and responsibilities assumed by the parties.	Customers are advised to assess the level of personal data protection provided by the countries involved in the data transfer and to formalize mechanisms for the cross-border transfer of personal data.

Core Requirements	Specific Requirements Applicable to Customer (As Data Processor)	Service Support Provided by HUAWEI CLOUD for Customers

Core Requirements	Specific Requirements Applicable to Customer (As Data Processor)	Service Support Provided by HUAWEI CLOUD for Customers
Obligations to process personal data	The customer shall not have any decision-making power regarding the scope and content of personal data processing activities and shall act only in accordance with the terms set by the data controller.	See section 5.1 "Obligations to process personal data
Use of subcontracting services	The provisions of this law that address the use of cloud computing by data controllers for personal data processing are the same as those of the Federal Act on the Protection of Privately Held Personal Data.	See section 5.1 "Use of subcontracted services
Protection of personal data	The Customer shall undertake to protect personal data in accordance with the principles and obligations set forth in this Law and the applicable regulations, as a prerequisite for the transfer of personal data outside the national territory of the Data Controller.	HUAWEI CLOUD provides customers with a variety of privacy protection technologies and services, including access control and identity authentication, data encryption, logging and auditing, to help customers protect their personal data according to their business needs.

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

HUAWEI CLOUD has a deep understanding of the importance of customers' privacy protection needs, combining it with its own privacy protection practices and technical capabilities in order to help customers to achieve compliance with the PDPA 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 Products**

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers (As Data Processor)
Identity and Access Management	Identity and Access Management (IAM) provides identity authentication and permissions	The Federal Law on the Protection of Personal Data held by Private

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers (As Data Processor)
(IAM)	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.	Parties (Article 19,21,22,23,24,25) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61,87,90) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,42,43,44,45,46,51,64,82)
Cloud Eye Service (CES)	Providing customers with a multidimensional monitoring platform for elastic cloud servers, bandwidth and other resources. Through Cloud Eye, 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.	The Federal Law on the Protection of Personal Data held by Private Parties (Article 20,22) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,43,44,45,46,51,64)
RDS for MySQL (RDS)	RDS for MySQL is a reliable and scalable cloud database service. Customers can deploy databases within minutes and stay focused on application development. • Customers can achieve fully managed software and hardware deployment, installing patches, automated backup, monitoring metrics, fast scalability, restore backup data and other functions through RDS, and ensure zero data loss in the case of high business load.	The Federal Law on the Protection of Personal Data held by Private Parties (Article 20,21) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61,64) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,40,42,82)
Elastic Cloud Server (ECS)	Elastic Cloud Server (ECS) provides secure, scalable, on-demand computing resources, enabling customers to flexibly deploy applications and workloads. • Through ECS, customers can realize multiple dimensions of security services such as Web application firewall and vulnerability scanning, realize security assessment of their own	The Federal Law on the Protection of Personal Data held by Private Parties (Article 20) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61,64) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 40)

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers (As Data Processor)
	cloud environment, realize intelligent process management based on customizable whitelist mechanism, and realize a number of scanning services such as general Web vulnerability detection and third-party application vulnerability detection.	

- **Security Products**

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers (As Data Processor)
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.	The Federal Law on the Protection of Personal Data held by Private Parties (Article 21) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,42,82)
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.	The Federal Law on the Protection of Personal Data held by Private Parties (Article 21) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,42,82)
Web Application	Web Application Firewall (WAF) can conduct multi-dimensional	The Federal Law on the Protection of Personal Data held by Private

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers (As Data Processor)
Firewall(WAF)	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.	Parties (Article 21) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,42,82)
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.	The Federal Law on the Protection of Personal Data held by Private Parties (Article 21) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,42,82)
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.	The Federal Law on the Protection of Personal Data held by Private Parties (Article 21) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,42,82)

- **Network Products**

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers (As Data Processor)
Virtual	Virtual Private Network (VPN)	The Federal Law on the Protection

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers (As Data Processor)
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.	of Personal Data held by Private Parties (Article 21) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,42,82)
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.	The Federal Law on the Protection of Personal Data held by Private Parties (Article 21) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,42,82)
API Gateway (APIG)	API Gateway is a high-performance, high-availability, and high-security hosting service that helps customers build, manage, and deploy APIs at any scale. Customers can protect API through identity authentication and permission control provided by APIG and implement flexible and quota management and throttling user requests to protect backend services, flexible and secure open service capabilities.	The Federal Law on the Protection of Personal Data held by Private Parties (Article 21) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,42,82)

- **Storage Products**

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers (As Data Processor)
Volume Backup Service	Volume Backup Service (VBS) creates online permanent incremental backup for cloud hard	The Federal Law on the Protection of Personal Data held by Private Parties (Article 21)

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers (As Data Processor)
(VBS)	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.	The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,42,82)
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.	The Federal Law on the Protection of Personal Data held by Private Parties (Article 21) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,42,82)
Object Storage Service (OBS)	Object Storage Service (OBS) provides stable, secure, efficient, and easy-to-use cloud storage service that lets customers store virtually any volume of unstructured data in any format and access it from anywhere using REST APIs. Customers can upload data through OBS encryption, authenticate the identity of users, and combine various methods and technologies to ensure the security of data transfer and access, and enable authentication protection for sensitive operations.	The Federal Law on the Protection of Personal Data held by Private Parties (Article 21) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article 31,42,82)
Elastic Volume Service (EVS)	Elastic Volume Service (EVS) provides persistent block storage, with advanced data redundancy and cache acceleration capabilities, EVS offers high availability and durability with an extremely low latency. Customers can use EVS encryption system disk and data disk, and the application of non-sensing, secure and convenient, can use the	The Federal Law on the Protection of Personal Data held by Private Parties (Article 21) The Regulation of the Federal Law on the Protection of Personal Data held by Private Parties (Article 50,52,59,61) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Article

Core Requirements	Specific Requirements Applicable to Customer (As Data Controller)	Service Support Provided by HUAWEI CLOUD for Customers (As Data Processor)
	distributed multi-copy technology, to ensure that any copy of the failure of rapid data migration and restoration, to avoid a single hardware failure caused by data loss.	31,42,82)

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, and ensure compliance with applicable laws and regulations. HUAWEI CLOUD's capabilities and achievements in privacy protection and personal data security have been widely recognized worldwide by third-party certifications. Up to now, HUAWEI CLOUD has obtained more than 20 certifications from more than ten organizations inside and outside China, including regional certifications on data security and global standard certifications related to privacy and data security.

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

- **SOC Audit**

  An independent audit report issued by a third party audit institution based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers. At present, HUAWEI CLOUD has passed the audit of SOC 1 Type II、SOC 2 Type II and released SOC 3 report.

Data Security Standard Certifications:

- ISO 27001 Information Security Management System Certification
- ISO 27017 Cloud Service Information Security Management System
- ISO 20000 Information Technology Service Management System Certification
- ISO 22301 Business Continuity Management System
- 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
- PCI 3DS supports the security standards implemented by 3DS
- TISAX (Trusted Information Security Assessment Exchange)

Regional Security Certifications:

- Multi-Tier Cloud Security (MTCS) Level3 (Singapore)
  - Association of Banks in Singapore (ABS) Outsourced Service Provider's Audit Report (OSPAR) (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 security, and respects and protects customer privacy rights. HUAWEI CLOUD has industry-leading 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 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 use of cloud services as appropriate and ensure compliance with the privacy protection laws and regulations of Mexico when using HUAWEI CLOUD.

8 Version History

Date	Version	Description
August 2024	1.1	Routine Update
November 2021	1.0	First release

